CHELTENHAM
BOROUGH COUNCIL

Notice of a meeting of Audit Committee

Wednesday, 23 March 2016
6.00 pm
Pittville Room - Municipal Offices

Membership	
Councillors:	Colin Hay (Chair), Chris Nelson (Vice-Chair), Matt Babbage, Flo Clucas, Dan Murch, David Prince and Pat Thornton

The Council has a substitution process and any substitutions will be announced at the meeting

Agenda

1.		**APOLOGIES**	
2.		**DECLARATIONS OF INTEREST**	
3.		**MINUTES OF THE LAST MEETING** 13 January 2016	(Pages 3 - 8)
4.		**PUBLIC QUESTIONS** These must be received no later than 12 noon on the fourth working day before the date of the meeting	
5.		**AUDIT COMMITTEE UPDATE** Grant Thornton (no decision required)	(Pages 9 - 26)
6.		**AUDIT PLAN 2015-16** Grant Thornton (no decision required)	(Pages 27 - 50)
7.		**ANNUAL INTERNAL AUDIT PLAN 2016-17** Audit Cotswolds (see recommendation)	(Pages 51 - 58)
8.		**INTERNAL AUDIT MONITORING REPORT** Audit Cotswolds (see recommendation)	(Pages 59 - 74)
9.		**ANNUAL RISK MANAGEMENT REPORT AND POLICY REVIEW** Corporate Governance, Risk and Compliance Officer (see recommendation)	(Pages 75 - 120)
10.		**REVISED CODE OF CORPORATE GOVERNANCE**	(Pages

		Corporate Governance, Risk and Compliance Officer (see recommendation)	121 - 140)
11.		**REVIEW POLICY GUIDELINES AND NEW POLICY AND PROCEDURES FOR THE ACQUISITION OF COMMUNICATIONS DATA USING THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)** Corporate Governance, Risk and Compliance Officer (see recommendations)	(Pages 141 - 212)
12.		**2020 VISION - RESIDUAL CORPORATE SERVICES** Corporate Governance, Risk and Compliance officer (no decision required)	(Pages 213 - 226)
13.		**WORK PROGRAMME**	(Pages 227 - 230)
14.		**ANY OTHER ITEM THE CHAIRMAN DETERMINES TO BE URGENT AND REQUIRES A DECISION**	
15.		**LOCAL GOVERNMENT ACT 1972 - EXEMPT INFORMATION** **The committee is recommended to approve the following resolution:-** "That in accordance with Section 100A(4) Local Government Act 1972 the public be excluded from the meeting for the remaining agenda items as it is likely that, in view of the nature of the business to be transacted or the nature of the proceedings, if members of the public are present there will be disclosed to them exempt information as defined in paragraph 5, Part (1) Schedule (12A) Local Government Act 1972, namely: Paragraph 5; Information in respect of which a claim to legal professional privilege could be maintained in legal proceedings	
16.		**APPROVAL OF EXEMPT MINUTES** 23 September 2015 (these were deferred from the last meeting as not all members had reviewed them prior to the last meeting).	(Pages 231 - 234)
17.		**DATE OF NEXT MEETING** 15 June 2016	
		Briefing notes (for information only) • Annual Governance Statement	

Contact Officer: Saira Malin, Democracy Officer, 01242 775153
Email: democratic.services@cheltenham.gov.uk

Audit Committee

Wednesday, 13th January, 2016
6.00 - 7.15 pm

Attendees	
Councillors:	Colin Hay (Chair), Chris Nelson (Vice-Chair), Matt Babbage, Flo Clucas, Dan Murch, David Prince and Pat Thornton
Also in attendance:	Peter Barber (Grant Thornton), Lucy Cater (Audit Cotswolds), Emma Cathcart (Counter Fraud Unit), Sarah Didcote (Deputy Chief Finance Officer), Jackson Murray (Grant Thornton) and Bryan Parsons (Corporate Governance, Rick and Compliance Officer)

Minutes

1. APOLOGIES
No apologies had been received.

Councillor Babbage arrived at 6:10pm.

2. DECLARATIONS OF INTEREST
No interests were declared.

3. MINUTES OF THE LAST MEETING(S)
The minutes of the previous two meetings had been circulated with the agenda.

Upon a vote it was unanimously

RESOLVED that the minutes of the meetings held on the 22 and 23 September 2015 be agreed and signed as an accurate record.

4. PUBLIC QUESTIONS
No public questions had been received.

5. EFFECTIVENESS OF THE AUDIT COMMITTEE
The Chairman explained that this item had needed to be deferred because the Officer who was going to deliver the presentation was absent due to sickness.

It was now likely that a separate session would be arranged in due course.

6. ANNUAL AUDIT LETTER 2014-15
Peter Barber of Grant Thornton introduced the Annual Audit Letter 2014-15 for Cheltenham Borough Council; which summarised the key findings arising from work carried out by Grant Thornton in year ending 31 March 2015. Members would be familiar with the detail contained in the letter as it summarised the details shared at the September 2015 meeting of the committee, but this was a far shorter report, aimed at key stakeholders. He reminded members that Grant

Thornton had issued an unqualified opinion on the Financial Statements Audit and Value for Money conclusion, at the 24 September 2014 meeting. The Audit fee for 2014-15 remained the same as originally disclosed in the 2014/-15 fee letter and audit plan and Appendix A; set out the issue and recommendation related to fixed assets, which had been discussed at length at the last meeting and included a management response.

He gave the following answers to member questions:

- Cheltenham was not alone; fixed assets were a problem area for a number of other authorities. Not only did they represent some of the largest figures for most council's, but many had been held for many years and many changes in approach to the valuations throughout that time. This was admittedly a very resource intense process for councils and he acknowledged that it was inherently difficult to accurately value fixed assets, but it was because of the volatility of the market, that they needed to be regularly valued.
- GCC and other higher tier authorities would have to include infrastructure assets (highways network assets) in their balance sheet for 2016/17 financial year.
- A piece of land would be valued based on where it was, what it was being used for and what was on it; trees themselves would not be given a value.
- Councils were required to demonstrate that they were making the best use of their assets and from Grant Thornton's perspective, assurances would be gleaned from whether the council had an up to date asset management plan, etc. It would be a democratic decision about whether income generation from assets was of more value than selling assets to realise their worth.

No decision was required.

7. CERTIFICATION OF GRANTS AND RETURNS 2014-15

Jackson Murray of Grant Thornton introduced the Certification letter for 2014-15. Despite a small number of relatively minor issues, set out at Appendix A, the claim had been qualified. The fee, which had previously been set by the Audit Commission, was now the responsibility of the Public Sector Audit Appointments (PSAA) and the 2014-15 fee was unchanged from the fee initially reported to the Audit Committee in the 2014-15 financial year.

It was noted that the DCLG website had been down since the end of November and Grant Thornton had therefore been unable, since that time, to complete certification. Members were assured that this was merely an administrative process and would be completed in due course.

There were no comments or questions on this item.

No decision was required.

8. AUDIT COMMITTEE UPDATE

Jackson Murray of Grant Thornton introduced the audit committee update as circulated with the agenda. The update was in the standard format and set out

progress as at the 22 December. It also included a summary of emerging national issues and developments and would inform the Audit Plan which was scheduled for consideration at the next committee meeting. He noted that the VfM criteria had changed for 2015-16 and now included; informed decision making, sustainable resource deployment and working with partner and other third parties. As always, Grant Thornton would adopt a risk based approach rather than looking at all areas in minute detail. Hard copies and/or links were available for each of the reports listed at the end of the update.

The following responses were given to member questions;

- The Business Location Index related to business growth in its totality; the number of businesses in an area and the direction of travel.
- Council tax collection rates across the country were at 97%, but this council had achieved 98% this year, for which those involved were to be congratulated. The council were considering increasing their council tax collection target to 98.75% for 2015-16, which was in itself; positive.

9. INTERNAL AUDIT MONITORING REPORT (INCLUDING COUNTER FRAUD UPDATE)

Lucy Cater, the Deputy Head of Audit, introduced the Internal Audit monitoring report, as circulated with the agenda. The report was designed to give the Audit Committee 'through the year' comment and assurances on the control environment at the council. The various appendices outlined progress against the Audit Plan, executive summaries for some of the reviews which had been concluded since the last meeting and also included a brief update on the Counter Fraud Unit. The team would soon begin planning for 2016-17 work and invited members to raise any topics for consideration.

The following responses were given to member questions;

- There was a shortfall in the recycling sale prices being achieved against those that were expected. The Section 151 Officer and Pat Pratley, as the Lead Commissioner, were both comfortable that the best prices were being achieved from what was a difficult market, given how values had dropped.
- Financial Rules state that a monthly reconciliation of the general ledger should be undertaken and this was found not to be the case in all but one of the four services that were reviewed. Whilst there was no evidence that monies had been misappropriated, this was the risk and reconciliation of the general ledger would allow for timely detection and investigation of any discrepancies. Some of the teams had already started to do monthly reconciliations but there was no suggestion that they would need to do retrospective reconciliations back to 2012.
- Work on the Contract Management review would be concluded in the next month and an Executive summary produced for the next meeting of the committee. Finance Officers were confident that the Purchase Order system was now being used as it should; though there were some areas which did not require a purchase order (grant payments, etc).
- HMRC could inspect the council at any time and VAT receipts would need to be produced in support of any expense claimed by Members for fuel. The VAT receipt simply needed to demonstrate that fuel had been

purchased and therefore did not need to be for the amount being claimed or indeed for the same day as the date of the claim.
- All of the organisations with which the council pooled money, were audited and the councils internal audit team sought assurances from the appropriate auditors where applicable. Members did feel however, that it would be useful to know how any findings were reported, in order to be able to decide what the Audit Committee might want to see going forward.

No decision was required.

10. COUNTER FRAUD AND ANTI-CORRUPTION POLICY

Emma Cathcart for the Fraud Unit, introduced the Counter Fraud and Anti-Corruption policy, as circulated with the agenda. The policy needed to be updated to reflect the changes to the counter fraud arrangements at the council, following the transfer of all benefit fraud investigation to the DWP and the formation of the counter fraud service on the 1 April 2015. The policy reflected the latest legislation and was developed to in consultation with all the Gloucestershire authorities and West Oxfordshire District Council. The policy was quite strategic in order that it would not need to be changed or revisited too regularly and the procedures that would support the policy were currently in the process of being drafted.

The following responses were given to member questions;

- The policy was based on the strongest parts of policies from this and the other authorities and reflected new legislation. A county wide approach to fraud investigation was unique to local authorities.
- Historically, authorities had shied away from focussing on corporate fraud, but this would become more important with an increasing number of shared services.
- Counter Fraud would be included in the updates presented to each meeting of the Audit committee and the team were keen to publicise any successful prosecutions, in partnership with the relevant authority's communications team.
- A policy was a policy, regardless of whether work was being undertaken for an authority within Gloucestershire or in another county, for West Oxfordshire District Council.
- Members were assured that, as a safeguard measure, RIPA applications would continue to be determined by this authority.

Upon a vote it was unanimously

RESOLVED that having considered the Counter Fraud and Anti-Corruption policy:

1. **No amendments are required to strengthen the Council's standards of propriety and accountability;**

2. **The Head of Audit Cotswolds, in consultation with the Section 151 Officer, be authorised to update the policy with any additional comments resulting from the ongoing counter fraud project.**

3. **The principles set out in the policy be supported by the committee and that the Audit Committee fulfil its role as set out in the policy.**

11. WORK PROGRAMME

The work programme had been circulated with the agenda.

No members raised any items to be included on the work plan.

12. ANY OTHER ITEM THE CHAIRMAN DETERMINES TO BE URGENT AND REQUIRES A DECISION

There were no urgent items for consideration.

13. LOCAL GOVERNMENT ACT 1972 -EXEMPT INFORMATION

Upon a vote it was unanimously

RESOLVED that in accordance with Section 100A(4) Local Government Act 1972 the public be excluded from the meeting for the remaining agenda items as it is likely that, in view of the nature of the business to be transacted or the nature of the proceedings, if members of the public are present there will be disclosed to them exempt information as defined in paragraph 5, Part (1) Schedule (12A) Local Government Act 1972, namely:

Paragraph 5; Information in respect of which a claim to legal professional privilege could be maintained in legal proceedings

14. EXEMPT MINUTES OF THE LAST MEETING

The exempt minutes of the last meeting had been circulated with the agenda.

Not all members had reviewed the exempt minutes on the restricted app on their iPad and therefore the chair deferred approval of this set of minutes until the next meeting of the committee.

15. DATE OF NEXT MEETING

The next meeting was scheduled for the 23 March 2016.

Colin Hay
Chairman

This page is intentionally left blank

Grant Thornton

Audit Committee Update

Cheltenham Borough Council

Year ended 31 March 2016

March 2016

Peter Barber
Engagement Lead
T +44 (0)117 305 7897
E Peter.A.Barber@uk.gt.com

Jackson Murray
Manager
T +44 (0)117 305 7859
E Jackson.Murray@uk.gt.com

Katie Haines
In Charge Auditor
T +44 (0)117 305 7697
E Katie.V.Haines@uk.gt.com

The contents of this report relate only to the matters which have come to our attention, which we believe need to be reported to you as part of our audit process. It is not a comprehensive record of all the relevant matters, which may be subject to change, and in particular we cannot be held responsible to you for reporting all of the risks which may affect your business or any weaknesses in your internal controls. This report has been prepared solely for your benefit and should not be quoted in whole or in part without our prior written consent. We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

.

Contents

Introduction

This paper provides the Audit Committee with a report on progress in delivering our responsibilities as your external auditors. The paper also includes:

- a summary of emerging national issues and developments that may be relevant to you; and
- a number of challenge questions in respect of these emerging issues which the Committee may wish to consider.

Members of the Audit Committee can find further useful material on our website www.grant-thornton.co.uk, where we have a section dedicated to our work in the public sector (http://www.grant-thornton.co.uk/en/Services/Public-Sector/). Here you can download copies of our publications including:

- Making devolution work: A practical guide for local leaders
- Spreading their wings: Building a successful local authority trading company
- Easing the burden, our report on the impact of welfare reform on local government and social housing organisations
- All aboard? our local government governance review 2015
- Knowing the ropes: Audit Committee effectiveness review
- Reforging local Government: financial health and governance review 2015

If you would like further information on any items in this briefing, or would like to register with Grant Thornton to receive regular email updates on issues that are of interest to you, please contact either your Engagement Lead or Audit Manager.

Peter Barber	Engagement Lead	T 0117 305 7897	M 07880 456122	Peter.A.Barber@uk.gt.com
Jackson Murray	Audit Manager	T 0117 305 7859	M 07825 028920	Jackson.Murray@uk.gt.com

Progress at 2 March 2016

Work	Planned date	Complete?	Comments
2015-16 Accounts Audit Plan We are required to issue a detailed accounts audit plan to the Council setting out our proposed approach in order to give an opinion on the Council's 2015-16 financial statements.	March 2016	Yes	The Audit Plan is a separate item on the agenda.
Interim accounts audit Our interim fieldwork visit includes: • updating our review of the Council's control environment • updating our understanding of financial systems • review of Internal Audit reports on core financial systems • early work on emerging accounting issues • early substantive testing • proposed Value for Money conclusion.	February – March 2016	Yes	We have completed our interim audit visit, and the key messages are included within our Audit Plan.
2015-16 final accounts audit Including: • audit of the 2015-16 financial statements • proposed opinion on the Council's accounts • proposed Value for Money conclusion.	July - August 2016	Not yet due	This work has not yet commenced.

Progress at 2 March 2016

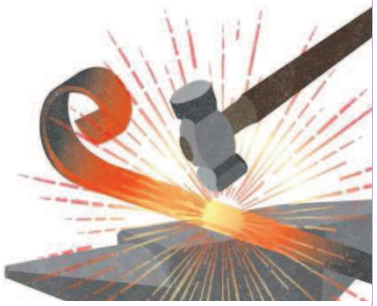
Work	Planned date	Complete?	Comments
Value for Money (VfM) conclusion The scope of our work to inform the 2015/16 VfM conclusion has recently been subject to consultation from the National Audit Office. The audit guidance on the auditor's work on value for money arrangements was published on 9 November 2015. Auditors are required to reach their statutory conclusion on arrangements to secure VFM based on the following overall evaluation criterion: *In all significant respects, the audited body had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.* To help auditors to consider this overall evaluation criterion, the following sub-criteria are intended to guide auditors in reaching their overall judgements: • Informed decision making • Sustainable resource deployment • Working with partners and other third parties. We will be required to report by exception if we conclude that we are not satisfied that the Council has in place proper arrangements to secure value for money in the use of its resources for the relevant period.	January – April 2016	Work is in progress.	The guidance and supporting information includes: • the legal and professional framework; • definitions of what constitute 'proper arrangements'; Guidance on the approach to be followed by auditors in relation to risk assessment, with auditors only required to carry out detailed work in areas where significant risks have been identified; • evaluation criteria to be applied; • reporting requirements; • LG specific guidance. The guidance is available at https://www.nao.org.uk/code-audit-practice/guidance-and-information-for-auditors/ Now that the finalised auditor guidance is available, we have carried out an initial risk assessment to determine our approach and have reported this in our Audit Plan. The findings from our work will be reported in the Audit Findings Report presented to the September meeting of the Audit Committee.

Reforging local government: Summary findings of financial health checks and governance reviews

Grant Thornton market insight

The recent autumn statement represents the biggest change in local government finance in 35 years. The Chancellor announced that in 2019/20 councils will spend the same in cash terms as they do today and that "better financial management and further efficiency" will be required to achieve the projected 29% savings. Based on our latest review of financial resilience at English local authorities, this presents a serious challenge to many councils that have already become lean.
Our research suggests that:

- the majority of councils will continue to weather the financial storm, but to do so will now require difficult decisions to be made about services
- most councils project significant funding gaps over the next three to five years, but the lack of detailed plans to address these deficits in the medium-term represents a key risk
- Whitehall needs to go further and faster in allowing localities to drive growth and public service reform including proper fiscal devolution that supports businesses and communities
- local government needs a deeper understanding of their local partners to deliver the transformational changes that are needed and do more to break down silos
- elected members have an increasingly important role in ensuring good governance is not just about compliance with regulations, but also about effective management of change and risk
- councils need to improve the level of consultation with the public when prioritising services and make sure that their views help shape council development plans.



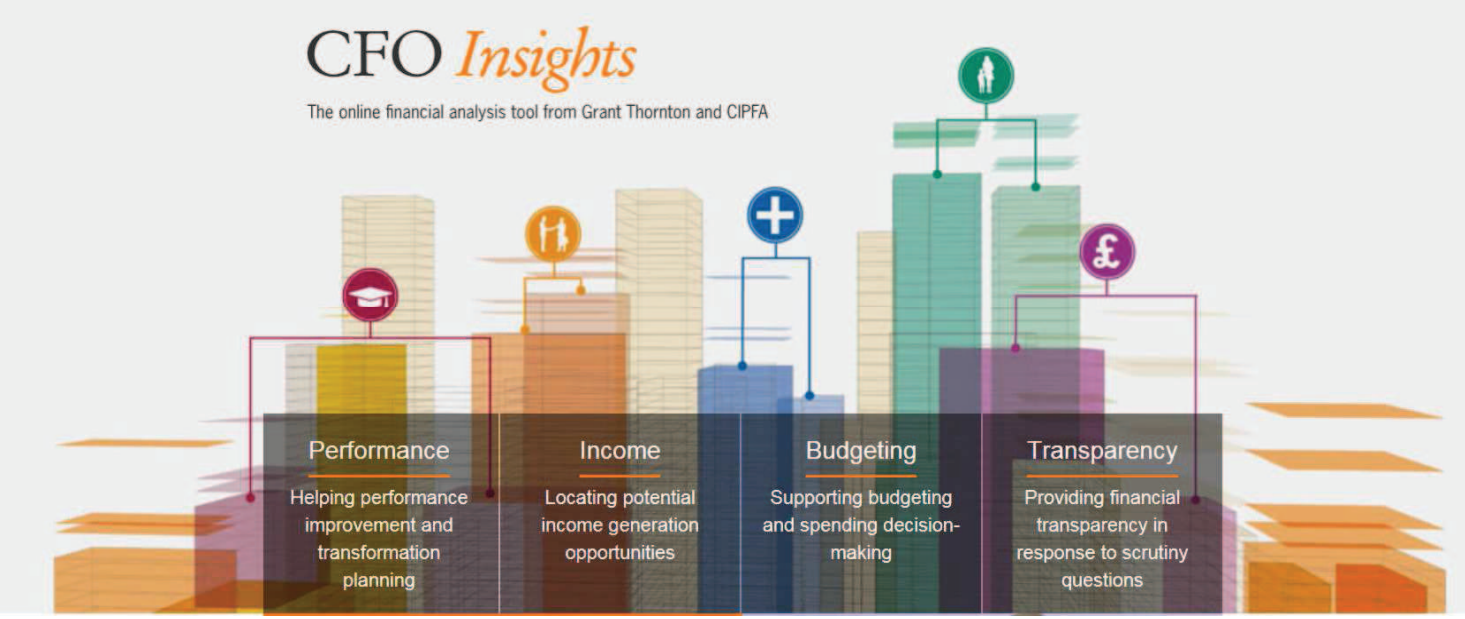
CFO Insights– driving performance improvement

Grant Thornton and CIPFA Market insight

CFO insights is an online analysis tool that gives those aspiring to improve the financial position of their local authority instant access to insight on the financial performance, socio-economic context and service outcomes of every council in England, Scotland and Wales.

The tool provides a three-dimensional lens through which to understand council income and spend by category, the outcomes for that spend and the socio-economic context within which a council operates. This enables comparison against others, not only nationally, but in the context of their geographical and statistical neighbours. CFO Insights is an invaluable tool providing focused insight to develop, and the evidence to support, financial decisions.

We are happy to organise a demonstration of the tool if you want to know more.
.



Local Authority Trading Companies

Grant Thornton Seminar - Building a successful local authority trading company

On 11th February Grant Thornton hosted a free client seminar, in Taunton, looking at Local Authority Trading Companies (LATC). It was attended by 29 officers from Councils in the South West. Although nobody from Cheltenham Borough Council could attend we would be happy to share our slides from the day with the Council.

As councils look for different ways to reduce costs, improve efficiency and generate income some are setting up local authority trading companies. We predict that the number of these companies will continue to grow over the next five years.

The seminar considered the themes set out in our recent report, 'Spreading their Wings', focusing on how to set up and build successful local authority trading companies.

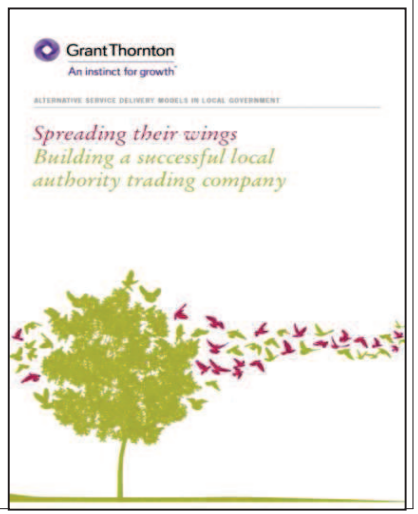
Attendees heard from Grant Thornton Local Government Advisory and Tax colleagues, with a focus on the complexities of Corporation tax, SDLT, VAT and Employment taxes when entering into such arrangements.

Martin Farrow from Buckinghamshire Care Limited shared his experiences from the Buckinghamshire Care journey "A merger between sustainability and purpose". He set the scene – underfunded social care, government savings, rising demand, and ageing population, service cutbacks mean a lot fewer people receiving services. The solution? A seismic shift in commissioning.

Hugh Lambourne from Bournemouth Borough Council explained his Council's approach to developing its commercial services "Building a successful LATC & Commercial Council". Offering an insight into why you might create an LATC or alternatively why you might choose not to trade through an LATC!

The day ended with a panel session with Martin and Hugh being joined by Sarah Longthorpe - Bournemouth Borough Council, Giles Letheren – Delt shared Services limited and Frank Wilson – Ubico Limited. A lively set of questions were posed by delegates.

Grant Thornton's next report on Joint Ventures will be available at the end of March.



Grant Thornton | An instinct for growth™

CIPFA reports and publications

Local Government Issues

Audit Panels

In December 2015 the Chartered Institute of Public Finance and Accountancy (CIPFA) published its guidance on the establishment of auditor panels.

Under the Local Audit and Accountability Act 2014 'relevant authorities' are able to appoint their own local auditors via an auditor panel. The Secretary of State for Communities and Local Government has decided to implement a phased introduction of the new local audit framework, with all health bodies and smaller local government bodies moving to the new framework as planned on 1st April 2017 and larger local government bodies a year later, on 1st April 2018. In practice, this means that smaller local authorities must have appointed their local auditors by 31st December 2016 and larger principal authorities by 31st December 2017.

The guidance sets out the options available to local authorities in England for establishing an auditor panel; what form such a panel can take; the operation and functions of the panel; and the main task of the panel – that is, advising the authority in connection with the appointment of the local auditor

Accounts - public rights of inspection and challenge

Local Government issues: National Audit Office

Council accounts: a guide to your rights

The NAO has published an updated version of Council accounts: a guide to your rights on its website. The guide has been updated to reflect the new requirements of the Local Audit and Accountability Act 2014, and applies to 2015-16 accounts. The document provides information on how people can ask questions and raise objections about the accounts of their local authority.

Arrangements for the exercise of public rights:

The Accounts and Audit Regulations 2015 set out new arrangements for the exercise of public rights from 2015/16 onwards. A key implication of the Act is that the final approval of the statement of the accounts by an authority prior to publication cannot take place *until after the conclusion of the period for the exercise of public rights*. As the thirty working day period for the exercise of public rights must include the first ten working days of July, authorities will not be able to approve their audited accounts or publish before 15th July 2016.

Smaller authorities must also wait until the conclusion of the thirty working day period for the exercise of public rights before publishing their accounts and the auditor's report.

Results of auditors' work 2014/15

Public Sector Audit Appointments

Following the closure of the Audit Commission on 31st March 2015, Public Sector Audit Appointments (PSAA) became responsible for appointing auditors to local Government bodies and for overseeing the delivery of consistent, high-quality and effective external audit services. The Audit Commission previously published Auditing the Accounts reports for Local Government bodies covering the 2012/13 and 2013/14 financial years. The reports summarised the results of the work of auditors appointed by the Commission at local bodies. This is the first such report published by PSAA, and it summarises the results of auditors' work at 509 principal bodies and 9,755 small bodies. The report covers the timeliness and quality of financial reporting, auditors' local value for money work, and the extent to which auditors utilised their statutory reporting powers.

The timeliness and quality of financial reporting for 2014/15 remained broadly consistent with the previous year for both principal and small bodies, according to Public Sector Audit Appointments Limited's *Report on the results of auditors' work 2014/15: Local government bodies*.

- for principal bodies, auditors at 345 of 356 councils (97 per cent) were able to issue the opinion on the accounts by the statutory accounts publication date of 30th September 2015.
- 97 per cent of police bodies and fire and rescue authorities also received the audit opinion by 30th September 2015.
- for the second year in a row there have been no qualified opinions issued to date to principal bodies.
- the number of qualified conclusions on value for money arrangements has remained consistent with the previous year at 4 per cent (17 councils, one police body and one fire and rescue authority).

IFRS 13 'Fair value measurement'

Accounting and audit issues

The 2015/16 Accounting Code applies IFRS 13 'Fair Value Measurement' for the first time. The standard sets out in a single framework for measuring fair value and defines fair value as the price that would be received to sell an asset or paid to transfer a liability (exit price) in an orderly transaction between market participants at the measurement date.

There is no public sector adaptation to IFRS13 but the Treasury and therefore the Code has adapted IAS 16 Property, Plant and Equipment so that operational assets (providing service potential) are no longer held at fair value but current value. As such IFRS 13 does not apply to operational assets. This new definition of current value means that the measurement requirements for operational property, plant and equipment providing service potential have not changed from the prior year.

However, surplus assets will need to be measured under the new definition of fair value, reflecting the highest and best use from the market participant perspective.

Other areas affected by the new standard include investment property, available for sale financial assets and those items where fair values are disclosed - for example, long term loans. IFRS 13 also introduces extensive disclosure requirements.

Local authorities need to:

- identify/ review their classification of surplus assets and investment properties
- discuss IFRS 13 with their property valuers and treasury advisers to ensure that fair values provided are produced in line with the new standard
- update accounting policies and disclosures to reflect the new standard.

Challenge question

- Has your Section 151 Officer reviewed the surplus assets and investment property categories to ensure what is included is correctly classified?
- Has your Section 151 Officer ensured property valuers and treasury advisers are aware of the fair value definitions under IFRS 13?
- Have the accounting policies and disclosures in your accounts been updated to reflect the IFRS 13 requirements?

Unlodged non-domestic rate appeals

Accounting and audit issues

Last year, there were primarily no provisions for unlodged non-domestic rates appeals as appeals received on or after 1 April 2015 were only backdated to 1 April 2015. The effect of last years announcement was supposed to put authorities in the position as if the revaluation had been done in 2015 as initially intended before the extension to 2017. This was only a one year reprieve and so any unlodged appeals at 31 March 2016 will only be backdated to 1 April 2015 and therefore may not be material.

However, this year, local authorities will need to estimate a provision for unlodged appeals but as above it may not be material.

Under IAS 37 'Provisions, Contingent Liabilities and Contingent Assets' and the Code it is in only extremely rare cases that a reliable estimate cannot be made. Therefore, if your local authority does have such an instance, the rationale needs backing up: both in terms of disclosures (as a contingent liability) and in providing evidence to those charged with governance as to why a reliable estimate for the provision cannot be made.

Challenge question

- Has your Section 151 Officer made plans to assess the need for an unlodged non-domestic rates appeal provision?

Website re-launch

Grant Thornton

We have recently launched our new-look website. Our new homepage has been optimised for viewing across mobile devices, reflecting the increasing trend for how people choose to access information online. We wanted to make it easier to learn about us and the services we offer.

You can access the page using the link below -

References

References

The reports and publications referenced within this update can be found using the following links. Hard copies of Grant Thornton publications can be obtained from your Engagement Lead or Audit Manager.

Reforging Local Government - http://www.grantthornton.co.uk/en/insights/reforging-local-government

Spreading their Wings – Building a successful Local Authority trading company - http://www.grant-thornton.co.uk/Global/spreading-their-wings-LATC-report-2015.pdf

National Audit Office 'Council accounts: A guide to your rights' - https://www.nao.org.uk/code-audit-practice/council-accounts-a-guide-to-your-rights/

Our new website can be accessed via http://www.grantthornton.co.uk/en/insights/?tags=local-gov&q=sustainable+communities

This page is intentionally left blank

The Audit Plan for Cheltenham Borough Council

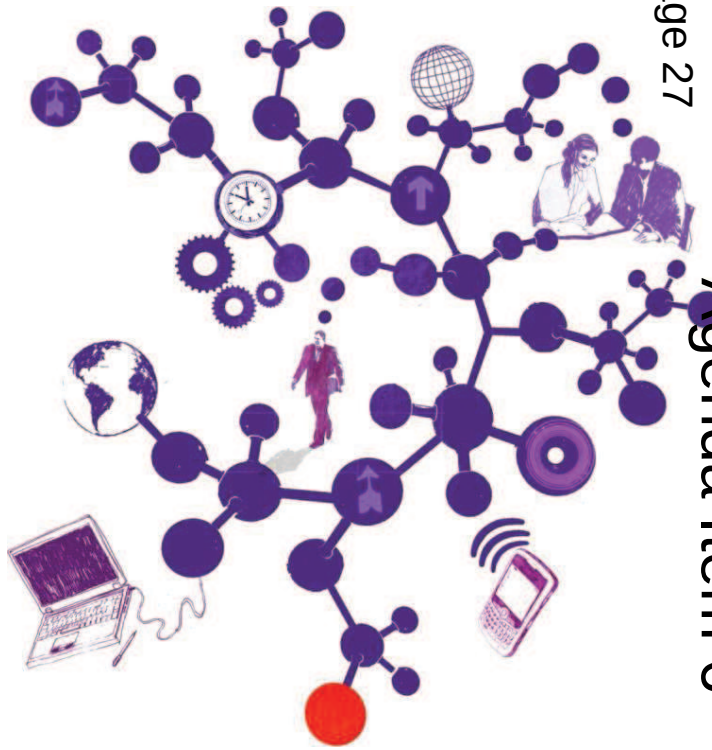
Year ending 31 March 2016

02 March 2016

Peter Barber
Engagement Lead
T 0117 305 57897
E peter.a.barber@uk.gt.com

Jackson Murray
Manager
T 0117 305 7859
E jackson.murray@uk.gt.com

Katie Haines
Assistant Manager
T 0117 305 7697
E katie.v.haines@uk.gt.com



The contents of this report relate only to the matters which have come to our attention, which we believe need to be reported to you as part of our audit process. It is not a comprehensive record of all the relevant matters, which may be subject to change, and in particular we cannot be held responsible to you for reporting all of the risks which may affect the Council or any weaknesses in your internal controls. This report has been prepared solely for your benefit and should not be quoted in whole or in part without our prior written consent. We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

Grant Thornton

Cheltenham Borough Council
Municipal Offices
Promenade
Cheltenham
GL50 9SA

Grant Thornton UK LLP
Hartwell House
55-61 Victoria Street
Bristol
BS1 6FT
T +44 (0) 117 305 7600
www.grant-thornton.co.uk

2 March 2016

Dear Members of the Audit Committee

Audit Plan for Cheltenham Borough Council for the year ending 31 March 2016

This Audit Plan sets out for the benefit of those charged with governance (in the case of Cheltenham Borough Council, the Audit Committee), an overview of the pla scope and timing of the audit, as required by International Standard on Auditing (UK & Ireland) 260. This document is to help you understand the consequences of ou work, discuss issues of risk and the concept of materiality with us, and identify any areas where you may request us to undertake additional procedures. It also helps us better understanding of the Council and your environment. The contents of the Plan have been discussed with management.

We are required to perform our audit in line with the Local Audit and Accountability Act 2014 and in accordance with the Code of Practice issued by the National Audit Office (NAO) on behalf of the Comptroller and Auditor General in April 2015.

Our responsibilities under the Code are to:

- give an opinion on the Council's financial statements
- satisfy ourselves the Council has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources.

As auditors we are responsible for performing the audit, in accordance with International Standards on Auditing (UK & Ireland), which is directed towards forming and expressing an opinion on the financial statements that have been prepared by management with the oversight of those charged with governance. The audit of the financial statements does not relieve management or those charged with governance of their responsibilities for the preparation of the financial statements.

Yours sincerely

Peter Barber

Engagement Lead

Contents

Section

Understanding your business

In planning our audit we need to understand the challenges and opportunities the Council is facing. We set out a summary of our understanding below.

Challenges/opportunities

1. Autumn Statement 2015 and financial health

- The Chancellor proposed that local government would have greater control over its finances, although this was accompanied by a 24% reduction in central government funding to local government over 5 years.
- Despite the announced increased ownership, the financial health of the sector is likely to become increasingly challenging.
- Cheltenham's Settlement Funding Assessment results in a fall in Government funding of 17.4% in 2016-17.

2. Devolution

- The Autumn Statement 2015 also included proposals to devolve further powers to localities.
- There has been a Gloucestershire wide devolution submission – 'We are Gloucestershire' - to Government, which was developed by the County Council, the six District Councils, the LEP, the PCC and the CCG.

3. Housing

- The Autumn Statement also included a number of announcements intended to increase the availability and affordability of housing.
- In particular, the reduction in council housing rents and changes to right to buy will have a significant impact on Councils' housing revenue account business plans.
- Cheltenham currently believe this change in policy will result in the loss of £6.691 million of income in the period to 2019-20, and assuming a return to previous policy of CPI +1% following the next four years, a loss of around £111 million over the next 30 years.

4. Joint arrangements

- Councils are involved in a number of pooled budgets and alternative delivery models which they need to account for in their financial statements.
- Cheltenham has a number of such arrangements in place which have helped deliver cost savings and service improvements over a number of years. These include UBICO, GO Shared Services, Cheltenham Borough Homes and more recently the Cheltenham Trust.
- The Council have entered into '2020 Vision' with Cotswold, West Oxfordshire and Forest of Dean Councils, with a Joint Committee established and first services set to transfer in April 2016.

Our response

- We will consider the Council's plans for addressing its financial position as part of our work to reach our VFM conclusion.

- We will consider your plans as part of the local devolution agenda as part of our work in reaching our VFM conclusion.
- We are able to provide support and challenge to your plans based on our knowledge of devolution elsewhere in the country.

- We will consider how the Council has reflected government announcements as part of its business planning process.
- We will share our knowledge of how other Councils are responding to these changes.

- We will review your proposals for accounting for these arrangements against the requirements of the CIPFA Code of Practice.
- We will consider the progress that has been made in relation to the 2020 Vision programme as part of our VfM conclusion.

Developments and other requirements relevant to your audit

In planning our audit we also consider the impact of key developments in the sector and take account of national audit requirements as set out in the Code of Audit Practice and associated guidance.

Developments and other requirements

1. Fair value accounting

- A new accounting standard on fair value (IFRS 13) has been adopted and applies for the first time in 2015/16.
- This will have a particular impact on the valuation of surplus assets within property, plant and equipment which are now required to be valued at fair value in line with IFRS 13 rather than the existing use value of the asset.
- Investment property assets are required to be carried at fair value as in previous years.
- There are a number of additional disclosure requirements of IFRS 13.

2. Corporate governance

- The Accounts and Audit Regulations 2015 require local authorities to produce a Narrative Statement, which reports on your financial performance and use of resources in the year, and replaces the explanatory foreword.
- You are required to produce an Annual Governance Statement (AGS) as part of your financial statements.

3. Earlier closedown of accounts

- The Accounts and Audit Regulations 2015 require councils to bring forward the approval and audit of financial statements to 31 May and 31 July respectively by the 2017/18 financial year.

4. Other requirements

- Cheltenham Borough Council are required to submit Whole of Government Accounts (WGA) consolidation pack which summarises the group accounts.

Our response

- We will keep the Council informed of changes to the financial reporting requirements for 2015/16 through ongoing discussions and invitations to our technical update workshops.
- We will discuss this with you at an early stage, including reviewing the basis of valuation of your surplus assets and investment property assets to ensure they are valued on the correct basis.
- We will review your draft financial statements to ensure you have complied with the disclosure requirements of IFRS 13.

- We will review your Narrative Statement to ensure it reflects the requirements of the CIPFA Code of Practice when this is updated, and make recommendations for improvement.
- We will review your arrangements for producing the AGS and consider whether it is consistent with our knowledge of the Council and the requirements of CIPFA guidance.

- We will work with you to identify areas of your accounts production where you can learn from good practice in other authorities.
- We will complete our work in advance of the current legislative timescales and will work with the Council to bring the audit dates forward in future years.

- We will carry out the specified audit procedures on Cheltenham's WGA consolidation pack on behalf of the National Audit Office.

Our audit approach

Global audit technology

Ensures compliance with International Standards on Auditing (ISAs)

- Understanding the environment and the entity
- Understanding the business
- Understanding management's focus
- Evaluating the year's results

→ Inherent risks, Significant risks, Other risks, Material balances →

Develop audit plan to obtain reasonable assurance that the Financial Statements as a whole are free from material misstatement and prepared in all material respects with the CIPFA Code of Practice on Local Authority Accounting using our global methodology and audit software

Note:
a. An item would be considered material to the financial statements if, through its omission or non-disclosure, the financial statements would no longer show a true and fair view.

Voyager

Creates and tailors audit programs

Stores audit evidence

Documents processes and controls

Materiality

In performing our audit, we apply the concept of materiality, following the requirements of International Standard on Auditing (UK & Ireland) (ISA) 320: Materiality in planning and performing an audit.

The standard states that 'misstatements, including omissions, are considered to be material if they, individually or in the aggregate, could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements'.

As is usual in public sector entities, we have determined materiality for the statements as a whole as a proportion of the gross revenue expenditure of the Council. For purposes of planning the audit we have determined overall materiality to be £1,644,000 (being 2% of gross revenue expenditure). We will consider whether this level is appropriate during the course of the audit and will advise you if we revise this.

Under ISA 450, auditors also set an amount below which misstatements would be clearly trivial and would not need to be accumulated or reported to those charged with governance because we would not expect that the accumulation of such amounts would have a material effect on the financial statements. "Trivial" matters are clearly inconsequential, whether taken individually or in aggregate and whether judged by any criteria of size, nature or circumstances. We have defined the amount below which misstatements would be clearly trivial to be £82,000.

ISA 320 also requires auditors to determine separate, lower, materiality levels where there are 'particular classes of transactions, account balances or disclosures for wh misstatements of lesser amounts than materiality for the financial statements as a whole could reasonably be expected to influence the economic decisions of users'.

We have identified the following items where separate materiality levels are appropriate.

Balance/transaction/disclosure	Explanation	Materiality level
Disclosures of officers' remuneration, salary bandings, members allowances and exit packages in notes to the statements	Due to public interest in these disclosures and the statutory requirement for them to be made.	£5,000
Disclosure of auditors' remuneration in notes to the statements	Due to public interest in these disclosures and the statutory requirement for them to be made.	£5,000

Significant risks identified

"Significant risks often relate to significant non-routine transactions and judgmental matters. Non-routine transactions are transactions that are unusual, either due to size or nature, and that therefore occur infrequently. Judgmental matters may include the development of accounting estimates for which there is significant measurement uncertainty" (ISA 315). In this section we outline the significant risks of material misstatement which we have identified. There are two presumed significant risks which are applicable to all audits under auditing standards (International Standards on Auditing - ISAs) which are listed below:

Significant risk	Description	Substantive audit procedures
The revenue cycle includes fraudulent transactions	Under ISA 240 there is a presumed risk that revenue may be misstated due to the improper recognition of revenue. This presumption can be rebutted if the auditor concludes that there is no risk of material misstatement due to fraud relating to revenue recognition.	Having considered the risk factors set out in ISA240 and the nature of the revenue streams at Cheltenham Borough Council, we have determined that the risk of fraud arising from revenue recognition can be rebutted, because: • there is little incentive to manipulate revenue recognition • opportunities to manipulate revenue recognition are very limited • the culture and ethical frameworks of local authorities, including Cheltenham Council, mean that all forms of fraud are seen as unacceptable.
Management over-ride of controls	Under ISA 240 it is presumed that the risk of management over-ride of controls is present in all entities.	**Work completed to date:** • Testing of journal entries in months 1-9 **Further work planned:** • Review of accounting estimates, judgments and decisions made by manageme • Testing of journal entries in months 10-12 and year end adjustments • Review of unusual significant transactions.

Significant risks identified (continued)

Significant risk	Description	Substantive audit procedures
Financial statement level risk arising from the systems upgrade of Agresso	The council uses Agresso as it's main financial system which was upgraded in February 2016. The upgrade involved data migration from the old system to the new system and therefore there is a risk of loss of data integrity.	**Work completed to date:** • Reconciliation of data prior and post implementation of system upgrade to ensure integrity of data transfer. **Further work planned:** • Our specialist IT Auditor will be conducting a review of the process and controls in April 2016.
Valuation of property, plant and equipment	The Council revalues its assets on a rolling basis over a five year period. The Code requires that the Council ensures that the carrying value at the balance sheet date is not materially different from current value. This represents a significant estimate by management in the financial statements.	**Work completed to date:** • Review of management's processes and assumptions for the calculation of the estimate. • Review of the competence, expertise and objectivity of any management experts used. • Review of the instructions issued to valuation experts and the scope of their work. .**Further work planned:** • Testing of revaluations made during the year to ensure they are input correctly into the Council asset register • Discussions with valuer about the basis on which the valuation is carried out and challenge of the key assumptions • Evaluation of the assumptions made by management for those assets not revalued during the year and how • Review and challenge of the information used by the valuer to ensure it is robust and consistent with our understanding. • Consideration of management's assertion that the current value of PPE assets not revalued as at 31 March 2016 are not materially different to their carrying value.

Significant risks identified (continued)

Significant risk	Description	Substantive audit procedures
Valuation of surplus assets and investment property	The CIPFA Code of Practice has implemented IFRS 13 for the 2015/16 financial statements. The Council is required to include surplus assets within property, plant and equipment in its financial statements at fair value, as defined by IFRS13. IFRS 13 also covers Investment Assets and Assets Held for Sale, which will need to be valued under the new provisions of IFRS 13. This represents a significant change in the basis for estimation of these balances in the financial statements. There are also extensive disclosure requirements under IFRS 13 which the Council needs to comply with.	**Work completed to date:** • Review of the competence, expertise and objectivity of any management experts used. • Review of the instructions issued to valuation experts and the scope of their work • Discussions with valuer about the basis on which the valuation is carried out and challenge of the key assumptions. **Further work planned:** • Review and challenge of the information used by the valuer to ensure it is robust and consistent with our understanding. • Review of management's processes and assumptions for the calculation of the estimate • Testing of revaluations made during the year to ensure they are input correctly into the Council's asset register • Review of the disclosures made by the Council in its financial statements to ensure they in accordance with the requirements of the CIPFA Code of Practice and IFRS 13.
Valuation of pension fund net liability	The Council's pension fund liability as reflected in its balance sheet represent significant estimates in the financial statements.	**Work planned:** • We will identify the controls put in place by management to ensure that the pension fund liability is not materially misstated. We will also assess whether these controls were implemented as expected and whether they are sufficient to mitigate the risk of material misstatement. • We will review the competence, expertise and objectivity of the actuary who carried out your pension fund valuation. We will gain an understanding of the basis on which the valuation is carried out. • We will undertake procedures to confirm the reasonableness of the actuarial assumptions made. • We will review the consistency of the pension fund asset and liability and disclosures in notes to the financial statements with the actuarial report from your actuary.

Other risks identified

"The auditor should evaluate the design and determine the implementation of the entity's controls, including relevant control activities, over those risks for which, in the auditor's judgment, it is not possible or practicable to reduce the risks of material misstatement at the assertion level to an acceptably low level with audit evidence obtained only from substantive procedures"(ISA (UK & Ireland) 315).

In this section we outline the other risks of material misstatement which we have identified as a result of our planning.

Other risks	Description	Audit approach
Operating expenses	Creditors related to core activities (e.g. supplies) understated or not recorded in the correct period	**Work completed to date:** • Documented our understanding of the controls operating in the operating expenditure system • Performed walkthrough to confirm that controls are operating as described • Understanding of the accruals process **Further work planned:** • Year end testing of creditor balance and accruals
Employee remuneration	Employee remuneration and benefit obligations and expenses understated	**Work completed to date:** • Documented our understanding of the controls operating in the employee remuneration system • Performed walkthrough to confirm that controls are operating as described • Trend analysis months 1-10 **Further work planned:** • Global reconciliation of employee remuneration system to general ledger • Trend analysis months 11-12

Other risks identified (continued)

Other material balances and transactions

Under International Standards on Auditing, "irrespective of the assessed risks of material misstatement, the auditor shall design and perform substantive procedures for each material class of transactions, account balance and disclosure". All other material balances and transaction streams will therefore be audited. However, the procedures will not be as extensive as the procedures adopted for the risks identified in the previous section but will include

- Heritage assets
- Investments (long term and short term)
- Cash and cash equivalents
- Borrowing and other liabilities (long term and short term)
- Usable and unusable reserves
- Movement in Reserves Statement and associated notes
- Statement of cash flows and associated notes
- Financing and investment income and expenditure
- Taxation and non-specific grants
- Segmental reporting note
- Officers' remuneration note
- Leases note
- Related party transactions note
- Capital expenditure and capital financing note
- Financial instruments note
- Housing Revenue Account and associated notes
- Collection Fund and associated notes

Other audit responsibilities

- We will undertake work to satisfy ourselves that disclosures made in the Annual Governance Statement are in line with CIPFA/SOLACE guidance and consistent with our knowledge of the Council.
- We will read the Narrative Statement and check that it is consistent with the statements on which we give an opinion and disclosures are in line with the requirements of the CIPFA Code of Practice.
- We will carry out work on consolidation schedules for the Whole of Government Accounts process in accordance with NAO instructions to auditors.
- We will give electors the opportunity to raise questions about the accounts and consider and decide upon objections received in relation to the accounts

Group audit scope and risk assessment

ISA 600 requires that as Group auditors we obtain sufficient appropriate audit evidence regarding the financial information of the components and the consolidation process to express an opinion on whether the group financial statements are prepared, in all material respects, in accordance with the applicable financial reporting framework.

Component	Significant?	Level of response required under ISA 600	Risks identified	Planned audit approach
Gloucestershire Airport	No	• A high level analytical review	• N/A	Desktop review performed by Grant Thornton UK LLP
Cheltenham Borough Homes	Yes	• Group instructions to be completed and sent to component auditor	• None	Full scope UK statutory audit performed by Grant Thornton UK LLP

UBICO Ltd

The structure of UBICO changed in 2015/16 with the addition of 3 more partners to the company. Membership is now made up of five partners – Cheltenham Borough Council, West Oxfordshire District Council, Cotswold District Council, Tewkesbury District Council and Forest of Dean District Council. The Council is currently reviewing the new arrangements in place to determine whether group accounts will be required in 2015/16.

The Cheltenham Trust

The Cheltenham Trust was established part way through the 2014-15 financial year. A review of the Trust against applicable accounting standards and the CIPFA Code of Practice on Local Authority Accounting is required by the Council to determine how the Trust should be treated in their statement of accounts.

Value for Money

Background

The Local Audit & Accountability Act 2014 ('the Act') and the NAO Code of Audit Practice ('the Code') require us to consider whether the Council has put in place proper arrangements for securing economy, efficiency and effectiveness in its use of resources. This is known as the Value for Money (VfM) conclusion.

The National Audit Office (NAO) issued its guidance for auditors on value for money work in November 2015 here.

The Act and NAO guidance state that for local government bodies, auditors are required to give a conclusion on whether the Council has put proper arrangements in place.

The guidance identifies one single criterion for auditors to evaluate:

> *In all significant respects, the audited body had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.*

This is supported by three sub-criteria as set out below:

Sub-criteria	Detail
Informed decision making	• Acting in the public interest, through demonstrating and applying the principles and values of good governance • Understanding and using appropriate cost and performance information to support informed decision making and performance management • Reliable and timely financial reporting that supports the delivery of strategic priorities • Managing risks effectively and maintaining a sound system of internal control.
Sustainable resource deployment	• Planning finances effectively to support the sustainable delivery of strategic priorities and maintain statutory functions • Managing assets effectively to support the delivery of strategic priorities • Planning, organising and developing the workforce effectively to deliver strategic priorities.
Working with partners and other third parties	• Working with third parties effectively to deliver strategic priorities • Commissioning services effectively to support the delivery of strategic priorities • Procuring supplies and services effectively to support the delivery of strategic priorities.

Value for Money (continued)

Risk assessment

We completed an initial risk assessment based on the NAO's guidance. In our initial risk assessment, we considered:

- our cumulative knowledge of the Council, including work performed in previous years in respect of the VfM conclusion and the opinion on the financial statements.
- the findings of other inspectorates and review agencies.
- any illustrative significant risks identified and communicated by the NAO in its Supporting Information.
- any other evidence which we consider necessary to conclude on your arrangements.

We have identified significant risks which we are required to communicate to you. The NAO's Code of Audit Practice defines 'significant' as follows:

> *A matter is significant if, in the auditor's professional view, it is reasonable to conclude that the matter would be of interest to the audited body or the wider public. Significance has both qualitative and quantitative aspects.*

We have set out overleaf the risks we have identified, how they relate to the Code sub-criteria, and the work we propose to undertake to address these risks.

Value for money (continued)

We set out below the significant risks we have identified as a result of our initial risk assessment and the work we propose to address these risks.

Significant risk	Link to sub-criteria	Work proposed to address
Medium term financial position The Council have been required to deliver substantial savings since 2010/11, and forecast continued significant savings requirements going forward. The current MTFP includes a balanced position for 2016-17, but includes a number of unidentified savings over the period to 2019-20.	Informed decision making Sustainable resource deployment	• Review of the MTFP, including the assumptions that underpin the plan. • Understand how savings are identified and monitored to ensure that they support the delivery of budgets.
2020 Vision The Council continues to progress the 2020 Vision partnership arrangement with Cotswold, West Oxfordshire and Forest of Dean District Councils. The success of 2020 Vision, through the members working together effectively, is critical to the medium term financial plan at Cheltenham.	Working with partners and other third parties	• Review of the progress made in the development of the 2020 Vision. • Understand how the Joint Committee is operating, how the Councils are working together to deliver planned savings.

Reporting

The results of our VfM audit work and the key messages arising will be reported in our Audit Findings Report and Annual Audit Letter.

We will include our conclusion as part of our report on your financial statements which we will give by 30 September 2016.

Results of interim audit work

The findings of our interim audit work, and the impact of our findings on the accounts audit approach, are summarised in the table below:

	Work performed	Conclusion
Internal audit	We have completed a high level review of internal audit's overall arrangements. Our work has not identified any issues which we wish to bring to your attention. We have also reviewed internal audit's work on the Council's key financial systems to date. We have not identified any significant weaknesses impacting on our responsibilities.	Overall, we have concluded that the internal audit service provides an independent and satisfactory service to the Council and that internal audit work contributes to an effective internal control environment. Our review of internal audit work has not identified any weaknesses which impact on our audit approach.
Entity level controls	We have obtained an understanding of the overall control environment relevant to the preparation of the financial statements including: • Communication and enforcement of integrity and ethical values • Commitment to competence • Participation by those charged with governance • Management's philosophy and operating style • Organisational structure • Assignment of authority and responsibility • Human resource policies and practices	Our work has identified no material weaknesses which are likely to adversely impact on the Council's financial statements
Walkthrough testing	We have completed walkthrough tests of the Council's controls operating in areas where we consider that there is a risk of material misstatement to the financial statements. Our work has not identified any issues which we wish to bring to your attention. Internal controls have been implemented by the Council in accordance with our documented understanding.	Our work has not identified any weaknesses which impact on our audit approach.

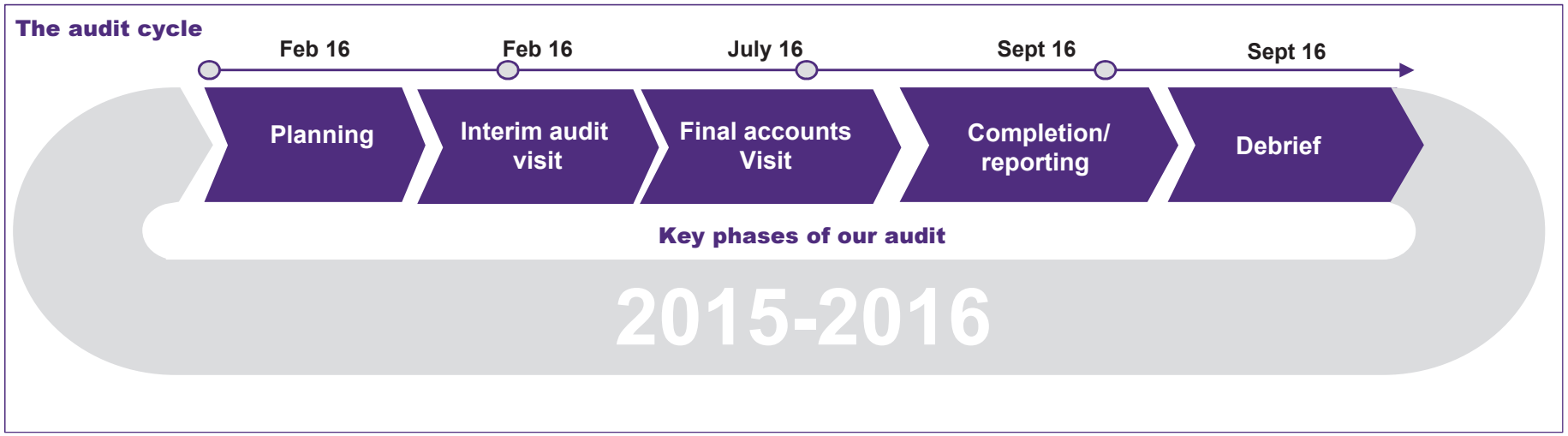
Results of interim audit work (continued)

	Work performed	Conclusion
Journal entry controls	We have reviewed the Council's journal entry policies and procedures as part of determining our journal entry testing strategy and have not identified any material weaknesses which are likely to adversely impact on the Council's control environment or financial statements. To date we have undertaken detailed testing on journal transactions recorded for the first ten months of the financial year, by extracting 'unusual' and 'large' entries for further review. No issues have been identified that we wish to highlight for your attention.	Our work has not identified any weaknesses which impact on our audit approach.
Early substantive testing	We completed early substantive testing on the following areas; • Operating expenditure transactions months 1-10 • Employee remuneration transactions months 1-10 • Property, plant and equipment existence testing • Property, plant and equipment rights and obligations testing • Balance sheet opening balances testing • Journals testing months 1-10 As in previous years, our testing has been undertaken as a joint effort between all applicable GO Shared Service partners to ensure the most efficient audit approach and to attempt to minimise any potential duplication of effort.	Our work has not identified any weaknesses which are likely to adversely impact on the Council's financial statements.

Results of interim audit work (continued)

	Work performed	Conclusion
Response to prior year actions	We reviewed the progress the Council has made against the prior year action plan where the following recommendations were made: • The Sections 151 Officer's ability to post journals should be removed • A review is undertaken of the effectiveness of the Fixed Asset Register due to issues identified in past two years relating to the Agresso fixed asset register module • The Council should ensure the 2015/16 Statement of Accounts are de-cluttered included a review of accounting policies to ensure they are applicable • Accounting policies should be reviewed and approved by members.	Our work has identified that: • The S151 Officer is no longer able to post journals • A review of the fixed asset register arrangements has been undertaken and for 2015/16 the asset register information is held and updated outside of the Agresso system. The audit team have reviewed the arrangements and are satisfied with the work and arrangements the Council have adopted. • The Council have began the process of reviewing the disclosures and accounting policies which will be included within the 2015/16 statement of accounts to ensure they are de-cluttered and appropriate. • Accounting policies have yet to be reviewed by members.

Key dates



Date	Activity
February 2016	Planning
February 2016	Interim site visit
March 2016	Presentation of audit plan to Audit Committee
July 2016	Year end fieldwork
September 2016	Audit findings clearance meeting with S151 Officer
September 2016	Report audit findings to those charged with governance (Audit Committee)
September 2016	Sign financial statements opinion

Fees and independence

Fees

	£
Council audit	£49,406
Grant certification	£8,361
Total audit fees (excluding VAT)	**£57,767**

Fees for other services

Service	£
Accommodation Strategy workshop	£3,000
Total fees for other services (excluding VAT)	**£3,000**

Our fee assumptions include:

- Supporting schedules to all figures in the accounts are supplied by the agreed dates and in accordance with the agreed upon information request list.
- The scope of the audit, and the Council and its activities, have not changed significantly.
- The Council will make available management and accounting staff to help us locate information and to provide explanations.
- The accounts presented for audit are materially accurate, supporting working papers and evidence agree to the accounts, and all audit queries are resolved promptly.

Grant certification

- Our fees for grant certification cover only housing benefit subsidy certification, which falls under the remit of Public Sector Audit Appointments Limited
- Fees in respect of other grant work, such as reasonable assurance reports, are shown under 'Fees for other services'.

Fees for other services

Fees for other services reflect those agreed at the time of issuing our Audit Plan. Any changes will be reported in our Audit Findings Report and Annual Audit Letter

Independence and ethics

We confirm that there are no significant facts or matters that impact on our independe auditors that we are required or wish to draw to your attention. We have complied with the Auditing Practices Board's Ethical Standards and therefore we confirm that we are independent and are able to express an objective opinion on the financial statements.

Full details of all fees charged for audit and non-audit services will be included in our Audit Findings Report at the conclusion of the audit.

We confirm that we have implemented policies and procedures to meet the requirements of the Auditing Practices Board's Ethical Standards.

Communication of audit matters with those charged with governance

International Standards on Auditing (UK & Ireland) (ISA) 260, as well as other ISAs, prescribe matters which we are required to communicate with those charged with governance, and which we set out in the table opposite.

This document, The Audit Plan, outlines our audit strategy and plan to deliver the audit, while The Audit Findings Report will be issued prior to approval of the financial statements and will present key issues and other matters arising from the audit, together with an explanation as to how these have been resolved.

We will communicate any adverse or unexpected findings affecting the audit on a timely basis, either informally or via a report to the Council.

Respective responsibilities

This plan has been prepared in the context of the Statement of Responsibilities of Auditors and Audited Bodies issued by Public Sector Audit Appointments Limited (http://www.psaa.co.uk/appointing-auditors/terms-of-appointment/)

We have been appointed as the Council's independent external auditors by the Audit Commission, the body responsible for appointing external auditors to local public bodies in England at the time of our appointment. As external auditors, we have a broad remit covering finance and governance matters.

Our annual work programme is set in accordance with the Code of Audit Practice ('the Code') issued by the NAO and includes nationally prescribed and locally determined work (https://www.nao.org.uk/code-audit-practice/about-code/). Our work considers the Council's key risks when reaching our conclusions under the Code.

It is the responsibility of the Council to ensure that proper arrangements are in place for the conduct of its business, and that public money is safeguarded and properly accounted for. We have considered how the Council is fulfilling these responsibilities.

Our communication plan	Audit Plan	Audit Findings
Respective responsibilities of auditor and management/those charged with governance	✓	
Overview of the planned scope and timing of the audit. Form, timing and expected general content of communications	✓	
Views about the qualitative aspects of the entity's accounting and financial reporting practices, significant matters and issues arising during the audit and written representations that have been sought		✓
Confirmation of independence and objectivity	✓	✓
A statement that we have complied with relevant ethical requirements regarding independence, relationships and other matters which might be thought to bear on independence. Details of non-audit work performed by Grant Thornton UK LLP and network firms, together with fees charged. Details of safeguards applied to threats to independence	✓	
Material weaknesses in internal control identified during the audit		✓
Identification or suspicion of fraud involving management and/or others which results in material misstatement of the financial statements		✓
Non compliance with laws and regulations		✓
Expected modifications to the auditor's report, or emphasis of matter		✓
Uncorrected misstatements		✓
Significant matters arising in connection with related parties		✓
Significant matters in relation to going concern		✓
Matters in relation to the Group audit, including: Scope of work on components, involvement of group auditors in component audits, concerns over quality of component auditors' work, limitations of scope on the group audit, fraud or suspected fraud	✓	✓

grant-thornton.co.uk

Cheltenham Borough Council

Audit Committee – 23 March 2016

Annual Internal Audit Plan 2016/17

Accountable member	**Cabinet Member Corporate Services, Councillor Jon Walklett**
Accountable officer	**Robert Milford, Head of Audit Cotswolds**
Ward(s) affected	**All**
Key/Significant Decision	**No**
Executive summary	The Council must ensure that it has sound systems of internal control which facilitate effective management of all the Council's functions. The work planned by Audit Cotswolds, the Council's Internal Audit service, is one of the control assurance sources to the Audit Committee and Senior Leadership Team and which supports the work of the external auditor. The work is also a key component of the Council's governance framework and as assurance source supporting the Annual Governance Statement, which forms part of the statutory accounting standards. Following CIPFA's guidance on Audit Committee the Committee this evening should "formally approve (but not direct) the Internal Audit plan".
Recommendations	**The Audit Committee approves the Internal Audit Plan for 2016/17**

Financial implications	The audit plan is a risk based plan which directs audits report towards the higher risk areas. This ensures that valuable audit resource is focused and directed towards ensuring that financial exposure is minimised. **Contact officers: Sarah Didcote and Paul Jones**
Legal implications	None specifically arising from the report recommendation. **Contact officer: Peter Lewis, Head of Legal Services, One Legal, peter.lewis@tewkesbury.gov.uk, 01684 272012**
HR implications (including learning and organisational development)	No HR implications **Contact officer: Julie McCarthy**

Key risks	The audit plan has been derived from consultation with the Senior Leadership Team and through reference to relevant policy, strategy and protocol documents including the risk register. The plan is designed to capture key and emerging risks that this Council faces over the year and therefore the plan will remain as flexible as possible to ensure internal audit resources remain focussed and valued. Internal Audit activity is needed each year to satisfy assurance requirements. For example, internal audit review key financial systems annually because the external auditors may rely on this in their own work on final accounts. In addition, the requirement for the Council to review its system of internal control and governance procedures means that assurance is required on systems and procedures relating to the compilation of the Annual Governance Statement. If this work is not completed by the Internal Audit additional fees from external audit may be incurred. Furthermore, Internal Audit is a statutory function under the Accounts and Audit (England) Regulations 2015. *"A relevant authority must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance."* The risk of failure to deliver core elements of the plan will be mitigated through the Partnership Board monitoring process. The representative from Cheltenham Borough Council is Paul Jones (GOSS Head of Finance (West) Section 151 Officer). Furthermore, Audit Committee will continue to receive quarterly reports through 2016/17 from Internal Audit detailing the work undertaken in relation to the plan.
Corporate and community plan Implications	None
Environmental and climate change implications	
Property/Asset Implications	None

1. Background

1.1 The environment in which Cheltenham BC and other Local Authorities now operates has presented significant drivers for change. The continual effort to meet the organisational objectives within a constrained budget has resulted in core systems coming under review for change. The introduction of GO Shared Service (GOSS) - a partnership arrangement for the delivery of core financial, human resources and procurement systems; the development of other shared services and now the 2020 Vision partnering arrangement all impact on service delivery processes and on core governance arrangements. Therefore, Internal Audit needs to be responding to the changing environment and the areas where the organisation now requires assurances. This reinforces the requirement for Internal Audit to follow a more flexible and risk based plan.

2. Reasons for recommendations

2.1 The primary role of Internal Audit is to provide assurance that the Council's systems constitute a proper administration of its affairs. To this end, Internal Audit carries out a programme of audits that is agreed annually with Heads of Service and the Executive Management Team and is approved by the Audit Committee.

2.2 The requirements of the Public Sector Internal Audit Standards (PSIAS) and changes of core systems Audit Cotswolds, as the Internal Audit provider, needs to respond to the changing environment and the areas where the organisation now requires assurances. This reinforces the requirement for Internal Audit to follow a more flexible and risk based plan.

2.3 The core financial systems delivered to the Council by the GOSS (now part of the 2020 Vision service delivery vehicle) are covered within the GOSS Audit Plan, this will cover GOSS and client side activities providing;

- Assurance to the GOSS Management Team and the Client Officer Group over the controls operating for the clients
- Assurance to the client (Cheltenham Borough Council) over the controls operating within GOSS financials, within the services they provide, and an assurance level for each financial module
- Assurance to the Council over the controls operating within service based activities associated with the financial processes administered by GOSS
- Periodic assurance over the other aspects of GOSS provided services
- The required support to the External Auditor

2.4 A summary of the Annual Internal Audit Plan for 2016/17 is included at Appendix 1. This lists the risk based assurance and consultancy work planned for the year. Counter fraud related audit work has not been included in this audit plan. Audit Cotswolds operate a specialised Counter Fraud Unit who will undertake proactive fraud reviews and also provide a reactive service to the Council should the need arise.

2.5 The Internal Audit Plan outlines a preferred programme of work for the year as developed throughout January and February 2016. The Audit Plan presented is not "set in stone" and is intended to evolve in response to issues highlighted through risk and change management and monitoring. Any changes to the agreed plan will only be made through a formal process involving the GOSS Head of Finance (West) & Section 151 Officer.

2.6 Audit Cotswolds has two further partners, West Oxfordshire DC and Cotswold DC and four further clients; Ubico, the 2020 Vision Partnership, Cheltenham Borough Homes and the Cheltenham Trust, so co-ordinating and allocating fixed resources across multiple organisations is critical to the success of the Audit Cotswolds Partnership and the delivery of all audit plans.

3. Consultation and feedback

3.1 The plan has been developed following consultation with and feedback from the Senior Managers, the Internal Audit Team and the Audit Committee.

4. Performance management –monitoring and review

4.1 The performance of Audit Cotswolds is monitored by both the Audit Committee and the Audit Partnership Board as detailed in the Audit Charter 2013.

Report author	**Contact officer: Lucy Cater Head of Internal Audit (Operational), lucy.cater@cotswold.gov.uk** **01285 623340**
Appendices	1. Internal Audit Annual Plan 2016/17 2. Risk Assessment
Background information	None

Appendix 1

Cheltenham Borough Council (CBC) Internal Audit Annual Plan 2016/17

Audit Theme / Service Area	Specific Topic or Activity	Audit Days
Section 1 - Core Governance and Core Finance Audits		**140**
Annual Governance Statement	Support for and review of the production of the Annual Governance Statement and sample elements of the supporting information	5
Audit Committee Effectiveness (Annual)	Annual review of the Audit Committee against appropriate guidance and standards	3
Internal Audit Self-Assessment (Annual)	Annual self-assessment of Internal Audit's performance against the Public Sector Internal Audit Standards (PSIAS)	2
Risk Management	Selection of risks from registers and mitigating controls and actions to test their effectiveness	5
ICT	Scope of 2016/17 to be confirmed	20
Council Tax Benefit	A review of an element of the Council Tax Benefit process, the programme of activity ensures full coverage of the service over a 3 year cycle	15
Council Tax	A review of an element of the Council Tax process, the programme of activity ensures full coverage of the service over a 3 year cycle	10
NNDR (Business Rates)	A review of an element of the NNDR process, the programme of activity ensures full coverage of the service over a 3 year cycle	10
GO Shared Service (GOSS) Audits	**Days allocated to the following Audits are CBC's element of the GOSS Audit Plan**	**70**
Main Accounting, Budgetary Control and Capital Accounting	A review of an element of the operating systems, the planned programme of activity ensures full coverage over a 3 year cycle. Assurances are sought for the GOSS controls operating in respect of its Clients and transactional testing is performed for each of the Clients	
Treasury Management and Bank Reconciliations		
Payroll		
Accounts Receivable (Debtors)		
Accounts Payable (Creditors)	Transactional Testing for each client, assurance over GOSS controls to be informed by SWAP auditors (the Forest of Dean DC's Internal Audit Team)	
Systems Administration of Agresso Business World (ABW)	A review of the operating system and the controls in place	
Human Resources	A review of a Human Resources area. Scope for 2016/17 audit to be determined with GOSS Officers	
Other GOSS Area	A review of Procurement / Health and Safety / Insurance. 2016/17 audit to be determined with GOSS Officers	
Section 2 - Risk Based Audits		**89**
Employee Turnover	Review of the controls in place to mitigate against loss of staff. How are management addressing the risk, identification of the reasons for staff turnover, are mitigating actions effective	10
Risk and Control Implications of Meeting the Funding Gap	Achievement of proposed financials in MTFS looking at the assessment of risks and achieving these projections (income / savings)	12
Garden Waste	Review of the processes and systems used for the charging of green waste. Looking at efficiencies, standardising processes etc.	8

Audit Theme / Service Area	Specific Topic or Activity	Audit Days
Business Rates Pooling	Audit of pooled assets (what / how / how are they reported), calculation of appeals. Suggestion from CBC Audit Committee	12
NNDR (Business Rate) Reliefs	Review of NNDR Reliefs ensuring that the correct relief has been added to accounts in accordance with legislation	12
Fleet Management	Review of the management of fleet by Ubico on behalf CBC (and CDC) to include the replacement of vehicles, purchase and recharging	10
Planning Application Process	Review of the planning application process to ensure compliance with statutory legislation in respect of the processing cycle	15
Food Safety	Review of the policies and procedures in place in respect of Food Safety to ensure compliance with the introduction of the new act which comes into effect from 1st April 2016	10
Section 3 - Advice and Consultancy		**114**
New Housing and Planning Act	Review of the introduction of the New Housing and Planning Act - ensuring the Council is ready / prepared for the new act	12
Community Infrastructure Levy (CIL)	Support for the CIL process ensuring that the Council is prepared for the introduction of CIL	10
Charging Mechanisms	Review of the charging mechanisms to include statutory and discretionary charges and the potential generating, or increasing income, from some service areas	15
Review of the outcomes of the Gloucestershire Joint Waste Committee	A review to ascertain if the Gloucestershire Joint Waste Committee is delivering the outcomes envisaged when it was established	12
2020 Vision Programme	Support for the 2020 Vision Programme and Projects	50
Change Programmes	Support for other change programmes / projects	15
Section 4 - Other		**57**
Management	Preparation of IA Monitoring Reports and preparation and attendance at Audit Committee. Annual Audit Planning. Attendance at Governance and Risk Groups. High level programme monitoring. Liaison meetings with CFOs and Management Teams.	15
Payment Channels and Income Streams Follow-Up	Follow-Up testing of a 'Limited Assurance' Audit	5
Follow Up Audits	Follow Up of Previous Year Audits	6
National Fraud Initiative	On-going Support for the Scheme	1
Contingency	New Work and Investigations	30
Total Number of Audit Days		**400**

Risk Assessment **Appendix 2**

The risk				Original risk score (impact x likelihood)			Managing risk				
Risk ref.	Risk description	Risk Owner	Date raised	Impact 1-5	Likeli-hood 1-6	Score	Control	Action	Deadline	Responsible officer	Transferred to risk register
Aud1	Without the audit plan in place there is the risk of insufficient audit work being completed to provide a reasonable assurance to stakeholders that there is an effective control framework in place, adequately mitigating risks to the authority's risk appetite.	GOSS Head of Finance (West) & Section 151 Officer		3	3	9	Reduce	The Audit Committee approval of the annual plan	31/03/2016	Head of Audit Cotswolds	
Aud 2	Without the delivery of the approved audit plan there is the risk of insufficient audit work being completed to provide a reasonable assurance to stakeholders that there is an effective control framework in place, adequately mitigating risks to the authority's risk appetite.	GOSS Head of Finance (West) & Section 151 Officer		3	3	9	Reduce	Appropriate support from service managers to aid the internal audit team in the delivery of its work. Monitoring of the delivery of the internal audit plan by; the Audit Partnership Board, the GOSS Head of Finance (West) & Section 151 Officer and the Audit Committee.	31/03/2017	Head of Audit Cotswolds	

This page is intentionally left blank

Cheltenham Borough Council

Audit Committee – 23 March 2016

Internal Audit Monitoring Report

Accountable member	Cabinet Member Corporate Services, Councillor Jon Walklett
Accountable officer	Robert Milford, Head of Audit Cotswolds
Ward(s) affected	**All**
Key/Significant Decision	**No**
Executive summary	The Council must ensure that it has sound systems of internal control that facilitate the effective management of all the Council's functions. The work delivered by Audit Cotswolds, the Council's internal audit service, is one of the control assurance sources available to the Audit Committee, the Senior Leadership Team and supports the work of the external auditor. The Annual Internal Audit Opinion presented to Audit Committee provides an overall assurance opinion at the end of the financial year. This Internal Audit Monitoring Report, however, is designed to give the Audit Committee the opportunity to comment on the work completed by the partnership and provide 'through the year' comment and assurances on the control environment.
Recommendations	**The Audit Committee considers the report and makes comment on its content as necessary**

Financial implications	None specifically arising from the recommendation **Contact officer: Sarah Didcote**
Legal implications	None specifically arising from the report recommendation. **Contact officer: Peter Lewis, Head of Legal Services, One Legal *peter.lewis@tewkesbury.gov.uk, 01684 272012***
HR implications (including learning and organisational development)	None specifically arising from the recommendation **Contact officer: Julie McCarthy**
Key risks	That weaknesses in the control framework, identified by the audit activity, continue to threaten organisational objectives, if recommendations are not implemented.
Corporate and community plan Implications	*"Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."* (*Chartered Institute of Internal Auditing UK and Ireland).* Therefore the internal audit activity impacts on corporate and community *plans.*

Environmental and climate change implications	Relevant to particular audit assignments and will be identified within *individual reports.*
Property/Asset Implications	None specifically arising from the recommendation **Contact officer: David Roberts@cheltenham.gov.uk**

1. Background

1.1 The Annual Audit Plan 2015/16 was aligned with the corporate and service risks facing the Council as identified in the consultation with the Senior Leadership Team and supported by such systems as the risk registers. The role and responsibilities of internal audit reflect that it is there to help the organisation to achieve its objectives, part of the plan has been aligned to elements of this strategy. However, to inform the audit plan we have also reviewed other key documents, such as the Medium Term Financial Strategy, change programme agendas and updates to the business plan, many of which contain risk assessments

1.2 There is also a benefit to supporting the work of the External Auditor (Grant Thornton). This is in the form of financial and governance audits to support such activities as value for money.

1.3 The audit plan also considered risks that may evolve during the year. The consultation process has sought to identify these areas considering where internal audit could support and add value to the risk control process. This report identifies work we have completed in relation to the planned audit work.

2. Reasons for recommendations

2.1 The environment in which Cheltenham BC and other Local Authorities now operates has presented significant drivers for change. The continual effort to meet the organisational objectives within a constrained budget has resulted in core systems coming under review for change e.g. the GO Shared Services impacting on core financial systems and shared services generally impacting on core governance arrangements.

2.2 Therefore Internal Audit needs to be responding to the changing environment and the areas where the organisation now requires assurances. This prompts the requirement to keep to a more flexible and risk based plan.

2.3 It should also be recognised that the service is a partnership, so co-ordinating resources across multiple organisations is critical to the success of the partnership.

2.4 This report highlights the work completed by Internal Audit and provides comment on the assurances provided by this work.

3. Internal Audit Output

The internal audit service is continuing to review its operational procedures and processes to ensure they align with the Public Sector Internal Audit Standards (PSIAS).

3.1 In support of internal audit standards compliance, and to aid with the complexities of managing an internal audit service over seven clients, we are procuring an IT system. Audit management software systems have been demonstrated and tenders evaluated. A preferred supplier was selected by the project team and two members of the team have visited sites in order to see the preferred system in operation. We held a clarification meeting with the supplier's representatives and a final decision has been made and the contract awarded. We will now commence the design and build of the system to our specifications.

3.2 Background

Below summarises some of Internal Audit's work in progress to date:

Core Governance

Fieldwork on Governance Compliance has been completed, the report has been issued and we are awaiting Management response.

Risk Management audit has commenced.

Core Financials

Council Tax, NNDR, Benefits (across three councils) – work is progressing.

Treasury Management and Bank Reconciliation audit has been finalised. A **High** assurance has been given for Treasury Management and **Satisfactory** assurance given for Bank Reconciliation.

Transactional testing for Accounts Payable has been completed. The report has been finalised with GOSS Management Team.

Accounts Receivable audit has been finalised and a **High** assurance has been given.

Main Accounting audit has been finalised and a **High** assurance has been given to both Main Accounting System and VAT processes.

Payroll report is being drafted.

Risk Based

Contract Management – the Draft report is with IA Management for review.

Business Continuity Management, Accommodation Strategy & Property Management and Security audits (across three councils) are all in progress.

Task force review and Safeguarding – fieldwork has commenced for both of these audits.

3.3 Progress against the 2015/16 audit plan, updated with progress and assurances given, is set out in **Appendix 1.**

3.4 Executive summaries of finalised audits in can be found in **Appendix 2**

3.5 The assurance levels are set out in **Appendix 3**

3.6 The Counter Fraud update is in **Appendix 4**

Report author	**Lucy Cater, Head of Internal Audit (Operational)** **Lucy.cater@cotswold.gov.uk** **01285 623340**
Appendices	1. Audit Plan Progress 2. Executive Summaries 3. Assurance levels 4. Counter Fraud Update

Appendix 1

Subject	Outline	Status	Assurance
Performance Management		Draft report issued - currently with Head of Audit Cotswolds	
Governance Compliance – Members Allowances		Final	Satisfactory
Data Protection & Control of Data		Final	Satisfactory
Payment Channels & Income Streams		Final	Limited
Social Media		Final	Satisfactory
Transparency		Final	High
CORE GOVERNANCE			
Annual Governance Statement	Support and review of the AGS	Complete	Satisfactory
Risk Management	Review of the training for service managers	In progress	
Performance Management	Focus on performance of projects and programmes and in particular the role and responsibilities of SLT and Cabinet.	In progress	
Governance Compliance	HR policy application by service managers: • Recruitment & Selection including induction • Capability, Grievance and Disciplinary • Training schemes	Draft Report issued – awaiting Management response	
ICT	Application audits Shared service support and review		
CORE FINANCIALS			
NNDR	Year 2 module of 3 year programme	In progress	
Benefits	Year 2 module of 3 year	In progress	

	programme		
Council Tax	Year 2 module of 3 year programme	In progress	
GOSS - Finance	Review on: • Accounts receivable • Main Accounting • Treasury Management & Bank Reconciliation • Payroll • Accounts Payable (transactional testing)	Final Final Final Report being drafted Final	High High High Satisfactory
GOSS - HR	Review on: • Absence Recording • Staff Allowances • Shared Services Allowances • Job Evaluation Process	Draft memos being updated following Management review	
GOSS – Procurement, Insurance, Health & Safety	Procurement	To commence	
RISK BASED			
Ubico Client Function	Follow-up to the 2013 audit review with the addition of an examination of client side cost covering client services provided by Gloucestershire Waste Partnership	In progress	
Business Continuity Management	Overall plans, service plans and service manager engagement	In progress	
Accommodation strategy and property management	Review of strategy and property management	In progress	
Security	Review of buildings and personnel security	In progress	
Audit Committee Effectiveness	Review of Audit Committee against appropriate guidance and standards	Work deferred until after Elections	
Contract management	Review of key contracts including tender processes Plus review of contractor use	Draft Report with IA Management for Review	
Task force review	Review of processes and procedures used in the	Fieldwork	

	Cheltenham Development Taskforce project	commenced	
Safeguarding Adults and Children	Support the Safeguarding peer review and audit	Fieldwork commenced	
CONSULTANCY			
REST project support	Support and on-going advice regarding the REST project	On-going	
20:20 vision	Support and on-going advice regarding the 20:20 project	On-going	
Other change projects	Support for other projects	N/A	
Other Audit Work			
Management	Audit Committee, governance and risk groups, high level programmes, etc	N/A	
Follow-ups	Assessment of recommendation implementation	N/A	
Contingency	Operational contingency	N/A	
Art Gallery & Museum follow-up	Follow-up of the recommendations made in the Art Gallery report	In progress	
Car parking follow-up	Follow-up of the report submitted to Audit Committee in September 2015	Delayed due to long term absence of the Head of Audit Cotswolds. Follow up is planned to commence April 2016.	

Appendix 2

Executive Summary for Social Media	
Assurance	**Satisfactory**

Overview and Key Findings

This audit was carried out as part of the risk based audit programme planned for 2014/15 as approved by Audit Committee at Cheltenham Borough Council April 2014.

The purpose of the audit review is to provide Members and senior officers with sufficient levels of assurance that the social media risk management process and internal control framework are effective. Our work has identified certain areas of control weakness, therefore we have suggested recommendations to strengthen the overall control environment.

Background

Social media is the term used for online tools, websites and interactive media that enable users to interact with each other by sharing information. Social media increases the Council's audience, improves the accessibility of our communication and increases our community engagement. There are multiple examples where the use of social media by public sector organisations has had a positive impact on both community engagement and organisational reputation. CBC have a combined following on all social media platforms of approximately 8000 'followers/subscribers'. With this level of reach there are increased reputational risks for the Council which if not controlled, hold the potential to escalate beyond the Council's existing risk management procedures.

Key Recommendations

Social Media Guidance/Policy:

- The Council's Social media guidance documents were last reviewed in 2012, the guidance should be updated to include clear links to existing relevant ICT and HR policies with the information communicated to all staff
- Employees with personal social media accounts should take extra caution in their social media activities, particularly when the personal social media account makes clear that the individual is a Council employee.
- Guidelines on the 'liking'/'following' process for corporate social media accounts should be included in the updated Social Media Guidance.
- The approval process for the creation of service area accounts should be documented within the updated Social Media guidance.
- Social media guidance should be updated to outline security, password, and acceptable use guidelines for officers administering Council social media accounts on personal devices (smartphones, tablets, home computer etc.).

Review and update the Council's social media security, recovery and business continuity arrangements to address the following risk and control areas:

- All Council-owned social media accounts should be registered using a Council email address with key account details logged on a central register for business continuity and disaster recovery purposes.

Conclusion

Based on testing completed, we offer an audit assurance opinion level of **Satisfactory Assurance**. The system of expected control although sound, has elements of weakness thus increasing system objective risks. The implementation of recommended actions within this report will increase the assurance level of the Council's risk management and internal control of Social Media.

Management Response

I welcome this audit report into the council's use of social media that has found that the council uses multiple social media platforms to communicate with over 8,000 people with many examples of best practice and that overall our system of control is "sound". I am happy with the report's recommendations that we should update both the social media guidance for staff and our social media security arrangements so that we minimise any reputational or security risks from our continued use of social media.

Executive Summary for Data Protection	
Assurance	**Satisfactory**

Overview and Key Findings

Audit Objectives and Scope

This review was part of the 2014/15 audit plan agreed by audit committee. The audit was included in the internal audit plan to provide assurance over the systems of control and risk management for Data Protection at Cheltenham Borough Council. This audit focussed on 3 objectives:

i) The adequacy and effectiveness of internal controls operating in respect of Data Protection:

- Data privacy impact assessments linked to 3rd party access to council data.
- Security and access to data.
- The controlled movements and transfer of data.
- Registering of systems and the maintenance of the registration.

ii) To ensure that the processes are meeting the requirements of internal policy, procedural standards and targets:

- Policies and procedures in place to support effective management of Data Protection arrangements.
- Links to PSN requirements.
- Data protection roles including training & induction. Evidence of training and refresher training across all staff
- Liability for and ownership of data when it is used by a third party e.g. a 'contracted out service'.
- Links to records management

iii) To ensure that the processes are meeting external codes of practice, professional good practice and statutory regulations as applicable:

- Sharing of data.
- Data protection links to transparency requirements.
- Data request management / control & performance to local / national requirements.
- CCTV and recorded data.
- Data protection reporting processes.

Background

To deliver services effectively, the Council needs to collect, process and hold personal and sensitive data relating to past and prospective employees, suppliers, clients and customers. The Data Protection Act 1998 requires organisations which handle personal data to manage the information securely and responsibly (this includes the destruction of information held safely when no longer required). Data protection covers a vast range of areas across the organisation and therefore the scope of this audit represents areas of risk that have been agreed with management.

Overall Observations and Key Findings

We found strong and robust internal controls in place including policies, procedure, use of usernames, passwords and segregated levels of access. There are however, some areas of weakness and non-compliance with existing controls that if left unmonitored could increase the overall risk profile for the Council. Implementation of the audit recommendations will help to mitigate the stated risks.

The following high priority observation has been made:

1. There is the potential vulnerability of Council data leaving the organisation without appropriate encryption arrangements in place. It has been agreed with the Council's in-house IT provider for the existing internal controls around file uploading to be reviewed and strengthened where necessary.

The following medium priority recommendations have been made:

1. The Council should seek to align its Clear Desk and Clear Screen Policies with the Forest of Dean District Council, awareness of the benefits and best practice should be circulated to staff.
2. The confidential waste contract should be reviewed to ensure the current arrangements offer the greatest value for money, taking advantage of links with strategic partners.
3. The Council should proactively provide all staff with specific data protection training in addition to the existing ICT induction training, with refresher training available at appropriate intervals.

Conclusion

We have met our objectives by reviewing the systems of internal control and risk management in place for Data Protection in accordance with the scope agreed by management. We offer a **Satisfactory** level of assurance, the system of expected control although sound, has elements of weakness thus increasing system objective risks, and, compliance is generally good but there is evidence of non-compliance with some of the controls. Recommendations have been made, that if addressed should help to add value to the controls already in operation.

Management Response

We have reviewed the Audit Report and agree with the observations and recommendations made. We will ensure the proposed actions are put into place to mitigate and manage the risk exposures identified.

Executive Summary for Accounts Receivable	
Assurance	**High**
Overview and Key Findings	

The Accounts Receivable (AR) review was conducted as part of the core audit programme for 2015/16 as approved by the relevant Audit Committees and Boards in March 2015.

This review will now be carried out over a 3 year cycle, with 2015/16 being the second year of this cycle. The focus of the review this year was on:

- Income Streams (Garden Waste, Trade Waste and Licensing processes)

The audit review also covered:

- The management of processes undertaken by GOSS on behalf of the client organisations
- That processes comply with Financial Rules and other Client based policies and standards
- An assessment of the GOSS performance levels and KPIs

Our review can confirm that sound processes and procedures are in place over the areas reviewed to ensure GOSS provides effective service delivery on behalf of the client organisations. We can also confirm that Financial Rules are being complied with as are client policies.

Examination of the Income Streams element of this review has identified that although processes undertaken by the GOSS AR team are sound, there are process inefficiencies for the administration of Green Waste Service. We also found errors made by client officers who have access to the Smart Client element of ABW. The relevant clients have been advised and the AR team are working to resolve the issues identified.

There are no KPIs in the 2015/16 GOSS Service Delivery Plan relating to the AR service, although there are internal performance schedules which form the basis for performance monitoring.

Other indications of GOSS performance is through (i) the monitoring/addressing of customer complaints; any performance concerns identified are reviewed and addressed for staff development, and (ii) the liaison meetings held between the GOSS AR Team and those service areas involved with the production of large subscription invoice runs. These discussions help to identify any issues / concerns to ensure the smooth running of the process. Our review of this area did not identify any areas of concern.

Based on the work completed, we can confirm that the control framework of the areas reviewed within GOSS AR is sound and that processes and procedures enable business objectives to be achieved. Several errors were identified within the client areas which The GOSS AR team are helping to correct to prevent further occurrences. One recommendation has been made that if addressed will add value and improve the overall control environment. Therefore, our opinion is that of a **High** level.

Management Response

We welcome the positive comments that have been made in relation to the current performance of the Accounts Receivable service.

The issues that have been raised relating to the service users are valuable points and we hope that these can be taken forward in future service specific audits to ensure that improvements can be made. GOSS AR will continue to support users and provide training when required. Some refresher training has already been arranged with staff at CBH.

The recommendation is in the process of being addressed. At present the system default is for the rounding to be on the last instalment. The user has to amend this to first at the point of setting up the payment plan. Advice is currently being sought from the System Administrator to see whether the default value can be amended from last to first. This would resolve the issue and the payment plan letter will display correctly.

Executive Summary for Accounts Payable (Transactional Testing)

Assurance	**Awaiting assurance score from SWAP**

Overview and Key Findings

The transactional testing for Accounts Payable (AP) was carried out as part of the core audit programme planned for 2015/16 as approved by the Audit Committees and Boards of the Audit Cotswolds' client organisations.
The South West Audit Partnership (SWAP) are the auditors for the AP module (GOSS Controls) as AP is processed by GOSS based at the Forest of Dean District Council (FoDDC) they also test the controls in place for the BACS payment batches. At the point of issuing this memo we have been advised that SWAP plan to commence the AP testing in January 2016 and we will receive a copy of their report (including the assurance level for the GOSS controls) once this has been completed.

In 2015/16 Audit Cotswolds performed AP transactional testing for all its clients and included:

- Payments are made in accordance with Financial Rules
- Appropriate authorisation of purchase orders and supplier invoices
- An assessment of the usage of Purchase Orders

We reviewed a random sample of invoices for the period 1st April – 30th September 2015. Where the sample did not contain individual transaction amounts falling within each approval limit, as stated by the Financial Rules, one additional transaction was randomly selected for each limit.

It's understood it is GOSS policy to make payment as soon an invoice is approved or matched to a purchase order. As part of this testing payments were deemed to be late if payment was made 30 days after an invoice was received by the service area. Our testing has identified 95% of invoices were paid within these 30 days, although not always within the supplier's terms set out on the invoice. We can confirm invoices had been authorised in line with the Financial Rules.

We are aware that a 'No purchase order, no payment' policy was approved by Senior Management Team at CBC (implemented April 2015), to increase the use of purchase orders and to ensure compliance with financial rules (although there are exceptions in the policy in respect of when a purchase order is not required e.g. utilities and subscriptions). Testing suggested that the policy has not increased the use of purchase orders during the first 6 months of this year. Consideration should be given to reminding officers of the policy and the potential lateness of payments to customers of non-compliance with this policy.

A further investigation to determine whether any invoices had been paid twice was undertaken for each client. Testing identified, in almost all incidences, duplicate payments were due to AP receiving duplicate copies of the invoice a few days apart, generally four to seven days; caused by service areas emailing the invoice and also submitting a paper copy. In all but one instance the invoice number on the second processed invoice was different to the first invoice number, which allowed the payment of the second invoice. The other invoice was processed twice as a different supplier ID had been used.

It was found that in the majority of cases the duplicate was approved by a different officer to the first, although there were two occasions when the approval was carried out by the same officer.

Conclusion

We can confirm that transactional testing has shown that invoices are paid in a timely manner, they are authorised appropriately and payments are made in accordance with the Financial Rules. Testing has identified there is still a need to increase the use of purchase orders by all clients to ensure compliance with Financial Rules.

There is a risk of making duplicate payments caused by AP receiving duplicate invoices, which could be avoided if all invoices are emailed rather than posted as discussed above.

Management Response

Since the inception of Accounts Payable being co-located in Coleford, performance levels of the timeliness in paying supplier invoices has improved year on year.

GOSS Management have put significant resource into training and reviewing processes for the use of purchase orders – it is therefore disappointing that this resource has not been rewarded with an improvement in the level of take-up in the use of purchase orders. Over the coming months, reports will be written to help establish which areas are not using the purchase order management element of the system to its full extent in order for Management Teams at clients to be able to 'police' the use more effectively.

Executive Summary for Main Accounting System & VAT Processes	
Assurance	**Main Accounting System – High** **VAT Processes – High**

Overview and Key Findings

The review on the Main Accounting System including VAT processes was conducted as part of the core audit programme for 2015/2016 as approved by the relevant Audit Committees and Boards of the Audit Cotswold client organisations.

The focus of the audit was on:

- The management of processes undertaken by GOSS on behalf of the client organisations: Cheltenham Borough Council (CBC), Cotswold District Council (CDC), West Oxfordshire District Council (WODC), the Cheltenham Trust, Ubico, and Cheltenham Borough Homes (CBH).

- Compliance of processes with Financial Rules and other client based policies and standards
- A follow up recommendations from the previous year's audit
- Review of Key Performance Indicators (KPIs) of GOSS performance

Based on the work completed we have concluded that there are sound controls operating within GOSS for the Main Accounting System, and with regard to VAT processes.

Our only comments relate to:

- the signing of VAT returns by the checking officer to evidence the check, and
- the development of ABW guidance resources and design of training materials

We have been able to issue High Assurance Level opinions for both the Main Accounting System and VAT processes. Other than the two issues mentioned above there are no other matters to which we need to draw the attention of management.

Management Response

Recommendations agreed, as per action plan.

Executive Summary for Treasury Management and Bank Reconciliation	
Assurance	**Treasury Management – High** **Bank Reconciliation – Satisfactory**

Overview and Key Findings

The review on Treasury Management and Bank Reconciliation was conducted as part of the core audit programme for 2015/2016 as approved by the relevant Audit Committees and Boards of the Audit Cotswold client organisations.

The focus of the audit was on:

- The management of processes undertaken by GOSS on behalf of the client organisations
- Compliance of processes with Financial Rules and other client based policies and standards
- A follow up recommendations from the previous year's audit

Based on the work completed we have concluded that there are sound controls operating within GOSS over Treasury Management activities and are able to offer a 'High' assurance opinion.

Original testing undertaken in October 2015 found that formal monthly bank reconciliation statements were not being completed although staff were identifying, examining and correcting un-reconciled items on an on-going basis. We were advised that a bank reconciliation template was being developed which has the facility to be signed off by the compiler and the verifier/certifier and would be shortly implemented. We revisited this in early January 2016 and found that work was still in progress. We subsequently revisited at the beginning of March 2016 and can confirm that monthly reconciliations are now being completed and there is evidence to support these reconciliations. But there is no evidence to support independent sign off of them. We understand the Corporate Finance Team are addressing this and will ensure a clear audit trail is progressed.

Due to the work now being undertaken by the Corporate Finance Team and our recent testing we are able to offer an assurance opinion to that of a 'Satisfactory' level. However, it must be noted that independent sign off of the bank reconciliation is a key financial control against fraud and error, so must be undertaken to provide assurance that the system is working effectively.

Management Response

Processes within the Treasury Management function are well established and are operating well. The recommendations made with regard to the Bank Reconciliation function are accepted and will be implemented shortly to further strengthen processes.

Appendix 3

Assurance Levels

Assurance levels for all audits follow a standard methodology to ensure reliability and validity of Internal Audit opinion. The table below set out the rationale for the opinion and suggested management action timescales.

Assurance Level	IA Opinion – Controls	IA Opinion – Compliance
High	The system of control is sound and designed to achieve system objectives	Controls are complete, consistently applied and compliance is good
Satisfactory	The system of expected control although sound, there are opportunities for improvement to further reduce system objective risks	Compliance is generally good but there is evidence of non-compliance with some controls
Limited	The system of controls falls below expectation as weaknesses are increasing system objective risks	There is sufficient evidence of non-compliance which puts the system objectives at risk
Poor	The system of control is weak thus significantly increasing system objective risk	There is significant non-compliance with controls leaving the system vulnerable to abuse or fraud which significantly increases the system objective risks

Appendix 4

Counter Fraud Update

Project Update for March / April Audit Committees

1. Cotswold District Council and West Oxfordshire District Council

S113 Secondment Agreements have now approved by appropriate legal teams and signed by all parties to enable both Counter Fraud Investigators to conduct work as needed for both authorities.

Two Cotswold cases of alleged theft and corruption against the Council are being investigated.

2. Cheltenham Borough Council

The Counter Fraud Officers currently undertake the single point of contact role and act as the Department of Work and Pensions liaison following the transfer of Benefit Fraud investigation to the Single Fraud Investigation Service, Department for Work and Pensions. The team also investigate any allegations related to Council Tax Reduction Scheme offences on behalf of the Revenues and Benefits Department. Agreed financial contribution made annually by the Council for this work – secured to 2020.

- 141 fraud referrals received
- 83 referred on to the single fraud investigation service for investigation
- 34 cases opened within the team
- 4 cases referred to a Housing Provider for further action
- Remaining 20 cases closed

Investigation cases involving Council Tax Reduction Scheme dealt with by the team

Overpayments identified (open cases after 01/04/15) = £16,737.95

- 3 prosecutions – all sentenced
- 2 prosecutions – listed for trial
- 2 Administrative Penalties (Fines generated for the Council £796.04)
- 2 Formal Cautions
- 5 on-going investigations

The Housing List review is almost complete and has resulted in 25 cancelled applications and 6 band reductions. Currently 150 queries are outstanding with Housing Options. Each cancelled application represents a property which can be reallocated to another eligible family. For each reallocation, a figure of £18,000.00 per annum can be identified as a loss avoidance figure because there is no need for temporary accommodation to be utilised.

A sample single person discount review has also been undertaken for the Revenues (Council Tax) Department. 50 cases were subjected to more robust verification; discounts were removed retrospectively and for the financial year 2016/2017 which generated £37,000.00 for the Council. Council Tax Penalties were not administered but could have been where appropriate generating £70.00 per account – approximately £3,000.00 in total.

Service of Court documents on behalf of Housing Benefit debt recovery:

- Customer debt of £634.28 paid in full
- Customer debt of £870 paid, arrangement agreed for outstanding £300
- Customer debt of £905.58, arrangement agreed & £211.30 paid to date
- Customer debt of £1858.46, arrangement of £40 per month agreed.

3. GO Shared Services

Sample of debts checked via the National Anti-Fraud Network to assist in debt recovery on behalf of the Accounts Receivable Team to reduce the number of debts passed for write off. This was a small sample of 24 cases to test the merits of Accounts having direct access to the system on behalf of each client Authority within GOSS.

Utilising only the free consent data check on the system, further information was found in 18 cases out of 24 – including email addresses, phone numbers and confirmation in many cases that the debtor was still resident at the address held, and also indications that some customers may have used a false name when

registering.

4. Internal Investigation Referrals
Internal Audit undertakes work for Cotswold, West Oxfordshire and Cheltenham – any internal cases referred to Internal Audit are referred to the team where criminal offences are identified. Reports and recommendations are being referred to the appropriate Director at suitable intervals.

5. Cheltenham Borough Homes
Tenancy Fraud work has been on-going for approximately 18 months. This has been successful and Cheltenham Borough Homes have contributed financially towards the fraud unit for 2015/2016.

- 2 Right to Buy Applications prevented
- 8 properties recovered
- 5 on-going investigations
- 5 prosecutions – all sentenced
- 2 prosecutions – listed for trial

A corporate strategy is being developed with regard to referral mechanisms, investigating and reporting.

6. Tewkesbury Borough Council
S113 Secondment Agreements have been approved by the appropriate legal teams and have been signed by all parties.

Work to commence with the Head of Revenues and Benefits and a retained Fraud Investigator with regard to the Housing List review and single person discount fraud drive in March 2016.

7. Gloucestershire County Council
Meetings held with the Head of Audit Risk Assurance and Insurance Services and key team members. The Head of Audit Risk Assurance and Insurance Services is a member of the Project Board.

S113 Secondment Agreements are with the legal department to enable the team to attend County and investigate reactive fraud cases as appropriate with a view to County pursuing prosecutions themselves. The County currently undertake a number of internal investigations but the cases are handed to the Police and the Crown Prosecution Service. The hope is that we can assist with this process being considered internally when appropriate.

8. Stroud District Council and Gloucester City Council
I have met with the Head of Internal Audit however he is leaving on 1 April 2016 and the service is joining with County. Therefore discussions to be held with the Chief Finance Officers following the commencement of the shared service to ensure both Councils are fully updated.

9. Forest of Dean District Council
A meeting with the Head of Internal Audit Team is to be arranged to discuss the project and appropriate engagement.

10. Housing Associations / Registered Social Landlord's
Severn Vale and Two Rivers have approached the team with regard to work. There is currently a work stream with the legal department to develop the best legal framework for this; either a Partnership Agreement or Goods and Services Contracts.

A meeting is to be planned in the new financial year to discuss tenancy fraud work with the team and liaison with Revenues and Benefits / Housing Teams within the authority.

11. Training
22 March 2016 - HR, Audit and Investigation staff across the County in relation to undertaking Employment / Internal Investigations,

Criminal Procedure and Investigations Act; refresher and updates being planned and rolled out across the County for all Enforcement, Legal and Audit members of staff (April / May 2016).

Regulation of Investigatory Powers Act; refresher and updates being planned and rolled out across the County for all Enforcement, Legal and Audit members of staff.

Proceeds of Crime Seminar planned provisionally for 3 May 2016 with Barristers from Albion Chambers for

all Enforcement, Legal and Audit members of staff across the County.

12. Data Warehouse / Case Management System

We are working with Procurement on the tender documentation – we are also discussing the project with the Head of ICT due to the size of IT involvement.

One Legal are being consulted with a view to drafting the legal documentation for data sharing / storing across the county.

This also involves a large work stream with regard to Fair Processing notices on the internet and paperwork across all partnership Councils.

13. Policies

Counter Fraud and Anti-Corruption Policy agreed by Audit Committee at Cotswold District Council and Cheltenham Borough Council; scheduled for 31 March 2016 at West Oxfordshire District Council.

Cabinet approval at Cotswold District Council received, on the agenda at Cheltenham and West Oxfordshire in April 2016.

A new Regulation of Investigatory Powers Act policy has been drafted to cover staff obtaining Communications data; approval across the partnership to be commenced

The team have been given responsibility for the Whistle Blowing Policy which needs to be redrafted for use across all partners. We are also looking at the Money Laundering and Proceeds of Crime Policies (if they exist).

14. Procedures

The investigation referral procedure needs to be worked on and adopted accordingly across the county and the partners.

We are working on a Lone Working Procedure for the team. We have researched and found appropriate lone working devices and pending legal agreement these will be obtained.

15. Other work streams

Work has also been planned in relation to a generic document pack for Gloucestershire for criminal investigation to include all the relevant investigation, interview under caution and prosecution processes.

A new referral inbox for county use; this will be advertised as we update the relevant intranet / internet pages to be used by staff, members or the general public. We are also trying to find an appropriate fix re telephone referrals.

Paperwork received in relation to signing the memorandum of understanding with HM Revenue and Customs – liaison with all enforcement teams.

A work stream to engage the Police and enter into an appropriate joint working mechanism is to be commenced.

Work on transparency reporting for fraud work – again this involves capturing information from around the organisations across the different sites.

Staff and Member Awareness Training Plan to be commenced.

16. Budget

This is now up to date for 2015/2016. Agreements for 2016/2017 to be finalised.

This page is intentionally left blank

Cheltenham Borough Council

Audit Committee – 23 March 2016

Annual Risk Management report and policy review

Accountable member	Cabinet Member Corporate Services, Councillor Jon Walklett
Accountable officer	Director Resources, Mark Sheldon
Executive summary	The Audit Committee approved the current Risk Management Policy March 2015 and requested an annual report to provide Members with an update on the Council's risk management activities.
Recommendations	That Audit Committee; 1. Note the risk management work undertaken during 2015/16. 2. Approve the Risk Management Policy for 2016-17 Appendix 2

Financial implications	None specifically arising from the recommendations. Contact officer: paul jones@cheltenham.gov.uk Tel: 01242 262626
Legal implications	None specifically arising from the recommendations. In general terms, the existence and application of an effective risk management policy assists prudent decision making which is less susceptible to legal challenge. Contact officer: peter.lewis@tewkesbury.gov.uk Tel: 01684 272012
HR implications (including learning and organisational development)	Risk management training for staff and elected members will be delivered through an e-learning tool on the Learning Gateway. Employees will be kept up to date on risk management progress and good practice through management meetings, team briefings and the intranet. Contact officer: Carmel Togher, HR Business Partner carmel.togher@cheltenham.gov.uk Tel: 01242 775215
Key risks	The lack of a robust approach to the management of risks and opportunities could result in ill-informed decision making and non-achievement of the Council's aims and objectives at both a strategic and service level.
Corporate and community plan Implications	None
Environmental and climate change implications	None

1. Background

1.1 Risk management is the culture, process and structures that are directed towards effective management of potential opportunities and threats to the Council achieving its priorities and

objectives.

1.2 Risk management is a key element of the Council's corporate governance framework. It is one of the six core principles of the Council's Code of Governance - 'taking informed transparent decisions which are subject to effective scrutiny and risk management'.

1.3 The Councils Risk Management Policy sets out the approach to risk management including the roles and responsibilities. The policy also details the processes in place to manage risks at corporate, divisional and project levels.

1.4 The Councils ICT services are managed through a partnership agreement; this includes the identification of risk and threats to our IT infrastructure and data and are managed in accordance to the requirements of the Public Sector Network framework. They are therefore not covered by the CBC Risk Management Policy but there are mechanisms in place to transfer share risks between 2020, ICT and CBC. e.g. through the Joint Management Board

1.5 In the past year, additional work has been completed to support the risk management process and help embed good practice across the council.

1.6 The Risk Management Policy was updated and approved by Audit Committee in March 2015 following a wide ranging review involving all elected Members and senior officers. The policy confirmed the Council's risk management appetite and objectives; links to the Council's Corporate Plan; and provides guidance on risk management approach and scoring.

1.7 The revised policy was made available to officers at Senior Leadership Team, Corporate Governance Group and at Divisional Management Team meetings. All policy, guidance and advice documents were updated and made available to all officers and elected Members through the risk management page on the intranet.

1.8 The Council has an on-line web based risk management module which records all corporate risk which can be used by all employees and Members helping to make risk management transparent.

Strategic risk management

1.9 The challenges facing Cheltenham Borough Council continue to intensify and the way that we meet these challenges creates the potential for increased opportunities and risk. The way that we address and mitigate the risks requires effective governance arrangements. Risk can be defined as the possibility of something happening, or not happening, that would have an impact on our ability to meet strategic or operational objectives.

1.10 The Council understands the importance of effective risk management and has a Corporate Risk Management Policy and an embedded risk management process.

1.11 The advantages of effective risk management are:

- helping to deliver strategic objectives and corporate priorities
- enabling better decision making
- facilitating effective control of budgets
- promoting better corporate governance
- Generating better value for money.

1.12 The identification and assessment of risk is part of the annual Corporate Strategy and Action Planning process. The Council's Senior Management Team considers and reviews strategic risks on a monthly basis. Both of these activities include the development of risk mitigation actions designed to reduce the likelihood and/or consequences of adverse events occurring. By understanding risks, the council can be more confident about undertaking ventures which produce

larger gains, such as jointly providing services with other councils.

1.13 The council's approach to risk management is overseen by the Audit Committee. This committee annually reviews the Risk Management Policy, considers internal audits reports on risk management, and also receives reports from external audit on the budget, accounts, grants and Value for Money.

1.14 In September and October of 2015 4 Councils made the decision to proceed with the 2020 programme which will lead to an increase in shared working activity between the partners to reduce costs and improve efficiency

1.15 The 2020 Vision Programme will be developing business plans for sharing services with our partner Councils to make the efficiency savings needed by each Council to maintain high quality services for their residents, and for their effective governance and decision making. All of these plans will be risk assessed and will be managed either by the 2020 Joint Management Board or CBC if they are retained.

1.16 In the near future each of the Councils and the 2020 Programme will need to review how risk assessment processes can be aligned and applied to corporate objectives, and programme projects and work streams. The Risk Management Policy at paragraphs 2.6 states that;

> *When we commission the delivery of a service or enter into a shared service/inter authority agreement, providers are obliged to have a range of risk management processes in place, should they identify a significant risk that may have an impact on the Council they must advise the Client Officer. The Client Officer will then decide on the best course of action. E.g. include on either the Corporate or Divisional Risk Registers.*
>
> *In addition we would expect all programme and project managers to assess the strategic and operational risks associated with the programme or project objectives before the project is selected and approved. Risks should be reviewed as the project proceeds and included within the Corporate Risk Register if the risk is likely to impact upon the authority as a whole.*

1.17 If the outcome of this review leads to any recommendations for amendments to the Councils Risk Management Policy to bring about a greater alignment of risk management they will be reported to Audit Committee for consideration and then to Cabinet for approval.

1.18 The 2015/16 Corporate Strategy set out our intended milestones, performance indicators and risks associated with delivering the Outcomes and the risks associated with their delivery. The Risk Management Policy states the need for a Corporate Risk Register (CRR) to identify risks associated with the achievement of the Council's aims and objectives within the Corporate Strategy. The CRR provides information on the risk description, scores, mitigation and the owners and managers. The CRR is reviewed by the Senior Leadership Team with copies provided to Cabinet every month. Directors discuss their risks with Cabinet Portfolio holders during their 1-2-1 meetings.

1.19 The on-line risk management module records all of the Council's corporate and Task Force risks which are initially identified by Directors and Service Managers; these are managed by an SLT appointed Risk Owner and Risk Manager or by the Task Force Risk and Accountability Group. Any divisional or project risk with a score of 16 or above must be referred to the Senior Leadership Team, they then consider if it should be escalated and recorded on the CRR. These corporate risks can also be referred back to the divisional or project risk registers if SLT consider the risks to be under control and less of a risk to the wider organisation.

1.20 As at 23/2/2015 there were 17 risks on the Corporate Risk Register compared to 15 in February 2016. During the period from April 2015 to February 2016, corporate risks were deemed to have been managed to the point where they had become acceptable and either closed or transferred by the Senior Management Team back to the division for ongoing management.

Internal Audit Recommendation

1.21 The overspend on the Art Gallery and Museum project resulted in the Audit committee commissioning Internal Audit to undertake a review as to "why" the overspend came about and to "identify" any improved processes to prevent it from happening again.

1.22 The Internal Audit review led to 8 recommendations, one of these was in respect of risk management and the need to enable a move to crises management should the need arise;

> *Recommendation 6.*
>
> *Risk management is the systematic process of understanding, evaluating and addressing these risks to maximise the chances of objectives being achieved and ensuring organisations, individuals and communities are sustainable. Risk management also exploits the opportunities uncertainty brings, allowing organisations to be aware of new possibilities. Essentially, effective risk management requires an informed understanding of relevant risks, an assessment of their relative priority and a rigorous approach to monitoring and controlling them.*
>
> *However, when the risk crystalizes a decision must be made to determine if it is significant enough to move to crisis management:*
>
> *Unlike risk management, which involves planning for events that might occur in the future, crisis management involves reacting to an event once it occurs. Crisis management often requires decisions to be made within a short timeframe and often after an event has already taken place.*
>
> *In project terms overspend, overtime, or unable to deliver objectives all should be considered triggers for crisis management. The Council should consider developing a crisis management plan for projects ensuring appropriate powers and accountability are given to the Officer appointed as the CMO (this role is therefore likely to be from the executive management level).*

1.23 This recommendation was considered as part of this year's review of the Risk Management Policy and it has been resolved that there should be not further amendment to the policy, the reasons for this are;

a) The current Risk management Policy already includes reference to risks classified as level 6 or Crises.

b) The current policy includes a process for continuing to challenge/review the scoring of risks, increasing the scores and for escalating them from divisional or project level to Corporate or Cabinet/Council

c) The other recommendations in the internal audit report included changes to;

d) communication process e.g. changes to risk assessments between project teams, Senior Leadership Team and elected Members - all of these have been implemented

e) defining roles and responsibilities i.e. who is responsible for the assessment and management of risk which has been implemented.

1.24 The Corporate Governance, Risk and Compliance officer has considered the current policy and the action taken in respect of addressing all of the other Internal Audit recommendations and concludes that there is no need for a new Crises Management process. This assessment is supported by the Acting Head of Internal Audit

Training

1.25 As part of awareness training for officers, risk management presentations have been completed at Senior Leadership Team and Divisional Management Team meetings to promote the Risk Management Policy and approach.

1.26 The on-line risk awareness training was updated to reflect the new policy and scorecard and this is available to all employees and Members through the Learning Gateway. A copy of the screen prints from this training module is attached at appendix 3.

Planned Improvements

1.27 The on-line risk management module can be developed further to include risks associated with key projects. These risks are currently managed by the project manager and reported to the programme board. A joint approach to risk management is planned for the 2020 partners so that there will be consistency in respect of the identification and scoring etc.

Policy review

1.28 The Risk Management Policy states the need for a formal review of the Corporate Risk Register to identify risks associated with the achievement of the Council's aims and objectives within the Corporate Strategy.

1.29 The Risk Management Policy was last reviewed and approved by the Audit Committee in March 2015.

1.30 The Risk Management Policy has been reviewed and considered by Corporate Governance Group and the Senior Leadership Team in February, there were no substantive recommendations for amendments except for;

1.31 the inclusion of the role and responsibilities of Overview and Scrutiny (para 10.7)

1.32 The broadening of the description in relation to how CBC risks are identified within the 2020 partnership and how they are transferred/escalated to the CBC CRR. (para 2.5)

1.33 . It is therefore recommended that Audit Committee also consider the policy and make any recommendations that it feels necessary or re-approve it for the 2016-17 year.

2. Alternative options considered

2.1 None

3. Consultation and feedback

3.1 The Senior Leadership Team and The Corporate Governance Group routinely consulted on the content of the risk registers.

4. Performance management – monitoring and review

4.1 The Senior Leadership Team and The Corporate Governance Group routinely monitor risks in line with the Risk Management Policy.

Report author	**Contact officer: Bryan Parsons** **Email: bryan.parsons@cheltenham.gov.uk** **Tel: 01242 264189**

Appendices	1. Risk Assessment 2. Risk Management Policy 3. Risk Management training slides from Learning Gateway

Risk Assessment

Appendix 1

The risk				Original risk score (impact x likelihood)			Managing risk				
Risk ref.	Risk description	Risk Owner	Date raised	Impact 1-5	Likeli-hood 1-6	Score	Control	Action	Deadline	Responsible officer	Transferred to risk register
	If the council does not have a robust and effective risk management approach to the management of risks and opportunities then it could result in ill-informed decision making and non-achievement of the Council's aims and objectives at both a strategic and service level.	Director Corporate Resources	23/03/2016	4	2	8	Reduce	Ensure that the Councils Risk Management Policy is kept up to date and that the processes supporting it are robust and delivered by the decision-makers.	31/3/2016	Corporate Governance, Risk and Compliance Officer	
	If the Council does not agree an aligned Risk Management Policy with the 2020 Joint Management Board then	Director Corporate Resources	23/03/2016	4	2	8	Reduce	Discuss with 2020 partners the development of a shared Corporate Risk Management Policy	31/3/2017	Corporate Governance, Risk and Compliance Officer	

	there is a risk that the risk assessment will become inconsistent										

Explanatory notes

Impact – an assessment of the impact if the risk occurs on a scale of 1-5 (1 being least impact and 5 being major or critical)

Likelihood – how likely is it that the risk will occur on a scale of 1-6

(1 being almost impossible, 2 is very low, 3 is low, 4 significant, 5 high and 6 a very high probability)

Control - Either: Reduce / Accept / Transfer to 3rd party / Close

CHELTENHAM
BOROUGH COUNCIL

www.cheltenham.gov.uk

Document control

Document Location; S:\Corporate\Risk\riskmanagementpolicy

Reviewed by; Audit Committee and Corporate Governance Group

Version Number	Version Date	Summary of Changes
1.0	14/02/2009	New Policy
1.2	19/04/2011	revised policy
1.3	23/01/2012	Draft Revised policy
1.4	01/04/2012	Confidential risks and new score card
1.5	01/04/2013	Additional requirement re commissioning
1.6	26/03/2014	Audit Committee
107	25/03/2015	Audit Committee
1.08	23/03/2016	Audit Committee

This document has been distributed to;	
Public website, Audit committee and Cabinet	1.0
Public website, Audit Committee and Cabinet	12 /04/2011
Audit Committee (agreed) All CBC staff, Public website and Cabinet members	21/03/2012
Audit Committee All CBC staff, Public website and Cabinet members	21/03/ 2013
Audit Committee All CBC staff, Public website and Cabinet members	26/03/2014
Audit Committee All CBC staff, Public website and Cabinet members	26/03/2015
Audit Committee All CBC staff, Public website and Cabinet members	01/04/2016

Index

Introduction to risk management cut out and keep section

The council believes that risks need to be managed, rather than avoided and that a rigorous approach to all aspects of risk management is an integral part of good management practice. Through having a sound risk management process we will ensure:

- That the council continues to achieve its objectives and outcomes and sustainable improvement in services;
- That the council is developing and maintaining a safe and healthy environment for the public, and for its employees; and
- That the council reduces the number and cost of insurance claims.
- That by mitigating risk we will make processes safer and more effective which in turn will reduce costs and make us more efficient.

Risk is defined in line with ISO 31000:2009 Risk Management Principles and Guidelines.

There are many definitions of risk and risk management. The contemporary definition set out in ISO 3100 is that risk is the "effect of uncertainty on objectives" where uncertainty can be either positive or negative.

Risk Management is defined as 'the culture processes and structures directed towards realising opportunities whilst managing adverse effects'. Its purpose is not to eliminate risk, but to understand it so as to take advantage of the upside and minimise the downside.

Everyone has a role to play in our risk management policy. Combining shared leadership with a team approach will help contribute to the success of integrated risk management.

Our expectations / commitments

- Senior Leadership team will own and maintain the corporate risk register which will be updated on a monthly basis.
- Directors will ensure that there is an up to date divisional risk register for their divisions using the template on the intranet. This should be reviewed at least quarterly at the divisional management team meetings. **Any divisional risk that has a score of 16 or greater will be referred to SLT** for consideration for inclusion on the Corporate Risk Register
- Service Managers will document risks to meeting their team objectives.
- All committee reports that require a decision should be accompanied by a risk assessment
- All project and programme mangers will assess the strategic and operational risks associated with the programme or project objectives.
- We will ensure that partnership working is part of our risk management approach; partnerships should identify the risks to achieving their objectives and the council will document the risks to working in partnerships.

Part One – Our approach to risk

1. Introduction

1.1 The aim of this policy is to set out Cheltenham Borough Council's approach to risk and the management of risk. It is presented in three parts; the first is our approach to risk management; the second outlines the process for risk management and the third part sets out roles and responsibilities.

1.2 The council believes that risk needs to be managed, rather than avoided and that a rigorous approach to all aspects of risk management is an integral part of good management practice. Through having a sound risk management process we will ensure:

- That the council continues to achieve its objectives and outcomes and sustainable improvement in services;
- That the council is developing and maintaining a safe and healthy environment for the public, and for its employees; and
- That the council reduces the number and cost of insurance claims.
- That by mitigating risk we will make processes safer and more effective which in turn will reduce costs and make us more efficient.

1.3 Risk is defined as

"An uncertain event or set of events which, should it occur, will have an effect upon the achievement of objectives, within the lifetime of the objective."

1.4 Risk can be both negative and positive, but it tends to be the negative side that we focus on and score. This is because some things can be harmful, such as putting lives at risk or a cost to an individual or the organisation in financial terms

1.5 Negative risk is represented by potential events that could harm the project. In general, these risks are to be avoided and can be measured in terms of impact and likelihood. Positive risk, on the other hand, refers to risk that we initiate because we see a potential opportunity, along with a potential for failure.

1.6 There are two examples of positive risks. The risk could either be a positive experience, or the reason for taking the risk has rewards that are well worth it. For example the risk could make us enhance our performance or reputation, or by taking a different option we could improve exceed corporate objectives, improve efficiency, reduce costs or improve income by a greater amount than was originally identified. See also section 8 about monitoring and managing risk.

1.7 Risk management is

"The activities required to identify and control exposure (negative risk) to uncertainty which may impact on the achievement of objectives". Or/and to use Positive risks to help us exceed our objectives.

1.8 From these two definitions, we can see that risk management is focused on the risk to meeting our objectives.

1.9 Given the definitions above, the council will assess, monitor and manage risks to the achievement of its objectives, including:

- Our corporate objectives – as set out in our corporate strategy;
- Divisional objectives;

- Service team objectives;
- Project and programme objectives; and

1.10 This policy sets out how we will identify, assess and manage risks, how we will report risk and how we will support risk management.

1.11 Everyone has a role to play in our risk management policy. Combining shared leadership with a team approach will help contribute to the success of integrated risk management. More information on roles and responsibilities is given in part 3.

2. Identifying, assessing and managing risks

2.1 The council will take a rounded view on what constitutes a risk. The starting point is that a risk could be anything, from an internal or external source, that poses a threat to the achievement of our objectives.

2.2 In terms of external sources, changing circumstances can have a significant impact on our ability to deliver our objectives. The environment we operate in is not stable and is in constant flux. Good risk management is about trying to anticipate these changes and put in place actions to respond to the resulting risks by minimising the likelihood and/or impact. Our view of the source of external risks could include the following:

- Local and national political change
- Local and national economic circumstance
- Social change
- Technological change
- Climate change
- Legislative change
- Environment
- Complying with equality considerations
- Change in the organisational structure for local government
- Changing expectations/needs from customer/citizens
- Change in how we are resourced
- Recommendations from assessment or review

2.3 In terms of internal source of risks, the ability of the council to continue to deliver its objectives is dependent on the following:

- Finance - sufficient finances in place to deliver service;
- Human resource - enough skilled, competent, experienced, healthy, motivated staff in the right place at the right time to deliver the service;
- Premises - the most appropriate environment from which to deliver the service;
- Technology – the most appropriate form of technology to support service delivery;
- Procurement – the most appropriate service/resource provider in place to deliver the service objectives (if service out-sourced);
- Legal/Contractual – the most appropriate form of contract to guide service delivery;
- Partners – commitment from appropriate other partners (both internal and external) to deliver the service;

- Changing priorities – a stable environment in terms of organisation priorities, clear objectives and manageable level of complexity;
- Information – an exchange of reliable information (internal and external) that is accurate and timely on which decisions can be fairly and correctly based.
- Safety and security of assets.

2.4 It is also worthwhile noting that because we have adopted a commissioning approach whereby the council may deliver services through different organisational models, and then we must ensure that these arrangements are included within our risk management processes. These risks can then be included in the same register as all other risks to the delivery of the objective. When it is necessary to the achievement of an objective to procure products and services, the risk/s to the objective if the procurement process fails should also be identified and managed. When these ownership and management mechanisms have been defined risk owners need to ensure that effective monitoring and governance controls are in place to protect council assets.

2.5 When we commission the delivery of a service or enter into a shared service/inter authority agreement, providers are obliged to have a range of risk management processes in place, should they identify a significant risk that may have an impact on the Council they must advise the Client officer. The Client officer will then decide on the best course of action. e.g. include on either the Corporate or Divisional Risk Registers.

2.6 In addition we would expect all programme and project managers to assess the strategic and operational risks associated with the programme or project objectives before the project is selected and approved. Risks should be reviewed as the project proceeds and included within the Corporate Risk Register if the risk is likely to impact upon the authority as a whole.

2.7 All committee reports that require a decision should contain a description of the options available and a risk assessment for each of them. These risks must relate to the objectives of the report topic.

2.8 Risk management should not be seen as a separate management function; it is a core part of good management.

2.9 The council have separate and detailed Health and Safety policies that provide advice about how this type of risks should be identified and managed. They can be found at safety policies and guidance | corporate pages on CBCi

2.10 Defining and scoring risk

2.11 Once risks have been identified using the information given above, the council would like risks to be defined in a consistent way using the “cause and effect” approach (see Part 2, 5.3 for more information). Risks will be then scored for impact and likelihood using the risk scorecard. (The risk score is the multiplication of impact and likelihood.)

2.12 The initial score will be based on current circumstances and referred to as the ‘original’ score. After controls have been actioned, the risk will be scored again. This score will be referred to as the ‘current’ score.

2.13 Tolerance and controls

2.14 The scored risk can then be assessed against the council’s tolerance levels. Currently we have three levels which set out the council’s attitude to that particular risk. The three tolerance levels are coloured red, amber and green. Risks that are scored in the red and amber areas (7 and above) will require action.

2.15 The council then has four options on how to control the risk;

- Reduce the risk
- Accept the risk
- Transfer the risk to a third party

- Close the risk

2.16 The decision on how to control the risk will be made by the risk owner or an appropriate senior officer depending on where the score falls in the tolerance areas and the costs associated with the control.

2.17 Monitoring and managing risk

2.18 As risk management is an integral part of good management all identified risks should be recorded and managed through either the Divisional Risk Register or the Corporate Risk Register. Corporate Risks are monitored monthly and Divisional Risk Registers will be monitored quarterly at routine Divisional Team meetings. **Any divisional risk that has a score of 16 or greater will be referred to SLT** for consideration for inclusion on the Corporate Risk Register

2.19 The Corporate Risk Register is available to all elected Members and employees through the intranet and is collectively monitored and managed by the Senior Leadership Team.

2.20 Recording risk

2.21 The risk registers should be used to inform decision making and resource allocation and should be updated as required to meet agreed monitoring arrangements.

2.22 Divisional Risk Registers are the responsibility of Directors with the individual risks being assigned to officers within the division (or across divisions where appropriate.)

2.23 Any new risk must be agreed by SLT before being added to the register. Risks cannot be deleted from the register unless they have agreed that it can be closed. Mitigating actions and deadlines can be updated by the risk owner at anytime prior to the monthly review at SLT.

3. Risk registers & reporting risk

3.1 The corporate risk register

3.2 The 'corporate risk register' contains strategic risks to the organisation

- The longer-term risks to the delivery of outcomes (ambitions) are described within the Corporate Strategy. The outcomes are linked directly to specific improvement actions which again are described within the Corporate Strategy but are individually risk assessed and managed within the Corporate Risk Register.
- Headline risks associated with exceptional circumstances.

3.3 Senior Leadership Team will own and maintain the corporate risk register and associated actions which will be considered and updated by them on a monthly basis.. A copy of the updated corporate risk register will be provided informally to Cabinet Members following review by SLT so that they can discus the risks with the risk owners or managers.

3.4 At every SLT meeting there is a standard agenda item that is called *Is it Safe* this provides all of the Directors with an opportunity to raise any new issue that they feel could have an impact on the Council. These issues are discussed and if necessary new risks are added either to the Project/Divisional Risk Register or the Corporate Risk Register

3.5 The corporate risk register will provide the necessary assurance for the annual governance statement.

3.6 An annual report (March) followed up by a six monthly risk monitoring report (September) to Cabinet

3.7 Risk management reporting should be co-ordinated with continuous routine performance monitoring.

3.8 All corporate confidential risks will be recorded in the normal way but they will be redacted either in full or in part from the corporate risk register so as to protect any personal data, prevent the disclosure of legally privileged information or exempt from publication any other information which should be so exempted. Further guidance on confidential risk can be found at paragraph 9.3.

3.9 Divisional, service area and team risk registers

3.10 Each division needs to take a proactive approach to risk management making sure that it is embedded as a part of the good management of the division. Each division should compile and maintain a divisional risk register that captures the risks to the delivery of its objectives.

3.11 Each service team, project/programme may also have a risk register which capture risks to their respective objectives. The important issue is to make sure that risk is discussed and debated at management teams and that risks are then identified and managed.

3.12 It is also important to note that those particularly high scoring divisional risks will not necessarily have a place on the corporate risk register unless it has a direct impact on our corporate objectives. In this case, the cause or effect may be different and the impact and likelihood scores must be scored appropriately. If the overall score for a divisional or project risk is 16 or over then it must be brought to the attention of SLT for consideration for inclusion on the Corporate risk Register.

3.13 It is possible that the same risk will appear in more than one register. The impact or likelihood may be different against the different objectives and should therefore be scored accordingly. Where actions to control a risk fall to another division, it is that division's responsibility to implement that action and the risk owner's responsibility to remain updated and manage the risk accordingly.

3.14 Reporting risks

3.15 Monthly risk monitoring reports will be presented to the Senior Leadership Team, and informally to Cabinet Members for discussion with Risk Owners. There will be an annual report to Cabinet and to Audit Committee which will include:

- The most significant corporate risks faced by the council;
- The associated management actions which are considered urgent;
- The resource implications of any management actions; and
- An overview of how significant risks may affect the Council's ability to meet its ambitions.

Risk management reporting should be co-ordinated with continuous routine performance monitoring.

4. Supporting risk management

4.1 Risk management co-ordination

4.2 The risk management policy, including any guidance notes, will be reviewed once a year by the Audit Committee and the responsible Director and when necessary, updated to incorporate further development in risk management processes and/or organisational change.

4.3 Where the council has established groups who have responsibility for risk, they should include detail about their role in the terms of reference or constitution for the group**.**

4.4 Training

4.5 The requirement for risk management training which will ensure that elected members and officers have the skills required to identify, evaluate, control and monitor the risks associated with the services they provide, or govern should be identified through the appraisal process.

4.6 Risk Management training for staff and elected Members will be delivered through an elearning tool on the learning gateway

4.7 Where required, training in corporate governance, of which risk management is a part, should be identified through the induction process for all new employees and members.

4.8 Communication

4.9 The risk management culture within the council must support open and frank discussion on issues that could put the Council at risk. Risk Owners and Risk Managers must provide opportunities to employees and members not normally involved with risk management with the opportunity for comment and challenge.

4.10 Risk should be considered at least quarterly by management team and service team meetings as part of good management practice. When necessary, new and emerging risks, significant change and where control actions are significantly succeeding or failing should be discussed.

4.11 It is the responsibility of the risk owner to communicate and discuss risk and control actions with other relevant officers, including those from other divisions.

4.12 If the cause of a risk or the failure of an objective or activity has the potential to impact on another objective or activity, it is the duty of the responsible officer to communicate that cause or failure to the owner of the effected objective or action.

4.13 Information and guidance on risk management will be available to all employees with computer access via the intranet and shared drive. Employees without computer access should speak to their manager for a printed copy.

4.14 Employees will be kept up to date on risk management progress and good practice through management meetings, team briefings and the intranet.

Part 2 - Process & Guidance

5. How to identify and define risks

5.1 Identifying risks is about asking:

- what could happen that would impact on the objective?
- when and where could it happen?
- how and why could it happen?
- how can we prevent or minimise the impact or likelihood of this happening?

5.2 What risks are identified and who you involve in the process will depend on whether you are looking at a specific team area or at a more strategic, organisational level. It is best practice to involve others in identifying risk as this gives you different perspectives on the same situation. Those involved must be clear about what objective is being risk assessed. Approaches to identify risks can include:

- Brainstorming on possible risks in a facilitated session;
- Mapping out the processes and procedures; asking staff to identify risks at each stage;
- Drawing up a checklist of risks and asking for feedback.

5.3 Risks should then be defined using the **'if ….. then** ….' (or the cause and effect or likelihood and impact) approach and given a reference number.

5.4 Risks should be specific and worded carefully and concisely and should not consist of a single word.

5.5 Risks should be outcome based and if one cause creates several impacts, each impact should be identified separately. This is because each might result in a different score and control.

6. How to score risk

6.1 The council has produced a scorecard to help risk owners score the risk by assessing impact and likelihood (effect & cause).

Impact

6.2 To help assess the impact (effect), we have identified a scale of impact from 1 to 5;

1) Negligible
2) Low
3) Moderate
4) Major
5) Critical

6.3 Risk owners are encouraged to decide the scale of the impact by considering what type of impact the risk has on the objective, using the risk types Financial, Employee, Capacity, VFM, H&S and wellbeing, Business continuity, Contractual Governance, Reputation, Customer satisfaction, Governance, Performance forecasting and Corporate Strategy. . A full description of impact type and scoring is detailed in the 'impact scorecard' which should be used when assessing risk.

Likelihood

6.4 To help the risk owner assess the likelihood score (cause), we have identified 6 categories of likelihood that the risk will occur during the lifetime of the objective. These are:

Score	*Likelihood*	*Probability*	*Action in response to risk levels*
1	Minimal	0-5%	Awareness of risk, no action
2	Very low	6-15%	Action to ensure likelihood does not increase
3	Low	16-30%	Preventative action required
4	Significant	31-60%	Minimise probability and/or impact
5	High	61-90%	Minimise probability and/or impact immediately
6	Very high	>90%	Plans made in advance must be carried out.

Risk score

6.5 The risk score is a multiplication of impact and likelihood.

6.6 On occasion it is possible to have a risk that proposes more than one score of impact, e.g. a single cause that could have minimal cost implications, maximum cost implications or anywhere in between. In this instance, we advise that you score and manage the risk according to the most likely scenario. Using the areas of tolerance may also help.

7. Selecting a risk control and understanding tolerance

7.1 The scored risk can then be assessed against the council's tolerance levels. Currently we have three levels which set out the council's attitude to that particular risk. The three tolerance levels are coloured red, amber and green. Risks that are scored in the red and amber areas (above 7) will require action.

Score	*Colour*	*Action/need to apply control*	*Responsibility*
1-6	Green	Acceptable, subject to monitoring.	Risk owner
7-15	Amber	Needs active management	Risk owner
16-24	Red	Requires urgent attention	Risk owner
25 - 30	Red	Requires urgent attention and routine discussion with Cabinet Leads	Risk Owner

7.2 The decision on how to control the risk will be made by the risk owner or an appropriate senior officer depending on where the score falls in the tolerance areas and the costs associated with the control.

7.3 The council has four options on how to control the risk;

Control	*Description*	*Tolerance area*
Reduce	The impact and/or likelihood needs to be reduced.	Amber or red
Accept	Impact and/or likelihood is at an acceptable level, it is impossible to reduce or is more cost effective to take the risk in not treating.	Amber or green
Transfer	Some of the risk is better controlled by an external partner. However some of the risk will remain (e.g. reputation) and that needs to be managed.	Any
Close	The risk has been terminated or is exceptionally low.	Green

8. Monitoring and managing risk

8.1 As risk management is a an integral part of good management our view is that risks should be reviewed by Senior Leadership Team and revised as and when actions prove to be successful or unsuccessful and when new information becomes available.

Progress of action	*Further action*
Positive but by a small margin	Current action not as effective as first hoped. Make changes or think of new action.
Positive by a significant margin	Current action successful – redirect resources.
Negative	Current action unsuccessful. Need new action.

8.2 The identification of risk may raise the question not to pursue a course of action. If this decision is made, it must be clearly documented.

8.3 The identification of risk may raise a success or positive learning point. This should be communicated to those who may benefit.

8.4 Actions to mitigate the risk need to be identified early and the monitoring must consider if they are being effective. If they are not then the project team, programme board or SLT need to identify new mitigating actions.

9. Risk registers

9.1 All risks will be recorded in either a Divisional Risk Register or a Corporate Risk register.

9.2 A risk register will record:

- Risks identified - to an objective, including a reference code and specified using "if…& then…";
- Original risk assessment and score based on impact and likelihood;
- Risk owner;
- Date raised;
- Control applied;
- Actions to control the risk;
- The officer responsible for the action;
- An indication as to whether the mitigating actions are on target
- The action status including progress notes;
- Current risk assessment and score once the action has been implemented.
- The date the risk was last reviewed

9.3 Confidential Risk

9.4 The Corporate Risk Register is a public document and is reported to Cabinet and Audit Committees. These reports may contain risks that contain confidential information and have been determined as being an "exempt item" under Schedule 12A of the Local Government Act 1972,

9.5 All corporate confidential risks will be recorded in the normal way but they will be redacted either in full or in part from the corporate risk register to ensure compliance with relevant legislation, to protect any personal or commercially sensitive data and the divulgence of any confidential legal advice.

9.6 Advice on the wording and inclusion of any confidential risks within the Corporate Risk Register must be sought from One legal.

9.7 The Senior Leadership Team may decide that they require additional assurance in respect of a particular confidential risk because it is not in the public domain, in which case it can be referred to the Corporate Governance group. Where they are referred they will be discussed with the risk owner and the outcome referred back to the SLT.

9.8 A process chart relating to the management of confidential risks is available on the Intranets Risk Management page.

Part 3 - Roles and Responsibilities

Everyone has a role to play in our risk management policy. Combining shared leadership with a team approach will help contribute to the success of integrated risk management.

10. Elected members

10.1 All elected members have risk management responsibility; they should promote the desired culture essential for successful risk management, acknowledging risk management as a strategic and operational tool to further the council's objectives. All should feel secure that, by identifying risk in their area, they are doing so within a corporate framework that is robust and easily understood.

10.2 The risk assessment included in all reports, that require a decision, that are brought to council, cabinet and committees should be used to inform decision making and should be revisited to ensure the risks are being managed.

10.3 They will also participate in training workshops to maintain an up-to-date understanding of how CBC manages risk.

10.4 Audit Committee

10.5 Audit Committee will endorse the council's corporate risk management policy, and at least annually, monitor and review the effectiveness of risk management systems and its contribution to corporate governance arrangements.

10.6 Audit Committee will also seek assurance from the internal audit team that risks are being managed in an appropriate manner and by the terms of this policy.

10.7 Overview and Scrutiny

The Overview and Scrutiny Committee may request to review the risk register at any time and scrutiny task groups may want to examine the any risks relating to a particular issue as part of a specific review. Any recommendations from scrutiny would be made to Cabinet or Council as appropriate.

10.8 Cabinet and Council

10.9 The Cabinet will approve the Risk management policy.

10.10 Cabinet and Council, as decision-making bodies, will be made aware of risks associated with any decision taken to them. They will have the responsibility to ensure that any risks to a report or project they sign off are managed and should request a revision of previously identified risks as and when necessary.

10.11 The Corporate Risk Register will be reported to Cabinet on a quarterly basis so that they can monitor the progress of mitigating action.

10.12 The corporate services cabinet member has risk management identified as part of their portfolio. They will have responsibility to ensure that their cabinet colleagues consider risk when setting policy and making decisions. These risks should be revisited to identify how they are being managed.

10.13 Individual cabinet members should seek assurance that the risk management process is being met in reference to their respective portfolios through discussions with Directors.

11. Officer responsibilities

11.1 The **Chief Executive** and **Executive Board** have strategic responsibility for the risk management policy and collectively oversee the council's effective management of risk. In their role as 'coach', they will advise and support Directors, Senior Managers, Programme and Project Managers to ensure that risk is managed consistently and in line with this policy.

11.2 The Executive Board are responsible for setting tolerance levels. The risk owner is empowered by Executive Board to make decisions about the control of the risk, depending on the risk score and what tolerance area it falls within.

11.3 They will consider corporate risk as part of developing and implementing the council business plan and corporate strategies, projects and programmes.

11.4 The **Senior Leadership Team** are collectively responsible for the management of risks recorded on the Corporate Risk Register

11.5 Directors are responsible for managing risks to the delivery of the objectives of their own division, jointly with their service managers. These risks will be managed in accordance with this policy, using the risk register template attached.

11.6 The **Director of Resources** is responsible for minimising the overall cost of insurance claims which do arise and supporting the risk management programme by supplying any advice and data to the Board.

11.7 The **Director of Resources** is responsible for monitoring the implementation and effectiveness of this risk management policy and for reviewing compliance with controls introduced by all other directors to collectively manage risks through the Senior Management Team. Any responsibilities delegated to internal audit will be covered in the annual internal audit programme.

11.8 The **Audit Partnership Manager** is responsible for ensuring that where corporate risks are identified in the Annual Audit Plan they are cross referenced to the Corporate Risk Register.

11.9 The **Client officer** for Shared or Commissioned Service(s) will be responsible for ensuring that any external organisation that provides a service(s) for the Council will have a documented Risks Management Process that is appropriate for the size and complexity of that organisation.

11.10 The Client Officer will ensure that any external organisations risk management process covered in 11.9 will include the process for that organisation to inform the Council of any risk that either impacts or could impact on the Council.

12. 'The Client Officer will make the appropriate ~~Senior Leadership Team~~ Lead Commissioner aware of any risk that could score 16 or above on the CBC score card or in their mind would have a significant risks to CBCs finances or reputation.'

12.1 The Corporate Governance Group

12.2 The Corporate Governance Group (CGG) is consulted on proposed amendments to the Risk management policy and the Corporate Risk Register.

12.3 The Senior Leadership Team can request that the CGG review and challenge any risk or group of risks to ensure that they are being recorded, scored and monitored correctly. This additional review process which can be found on the intranet relates to confidential risks and is designed to provide additional assurance to SLT and the risk owners that they are being managed correctly.

13. Programme and Project Managers

13.1 ensuring there is a process for identifying, managing and communicating risks to programme and project objectives and benefits

13.2 ensuring that programme and project teams carry out regular risk assessment

13.3 ensuring that risks are escalated to Corporate Risk Register where appropriate.

14. Service managers

14.1 **Service managers** are responsible for identifying and managing risks to the objectives of their service team in line with this policy. The council encourages managers to identify, understand and manage risk, and learn how to accept risk within the applicable tolerance level.

14.2 They should ensure that their teams carry out risk assessment, where appropriate, as a routine part of service planning and project management, including reporting to members.

15. All council employees

15.1 The identification of risk relies on input from teams and individuals.

15.2 A 'Risk Owner' is the owner of a risk and will manage that risk accordingly. This will involve maintaining awareness of how control actions are progressing.

15.3 All actions identified to control a risk will be assigned to an individual officer who will be called the action ‘Responsible Officer’.

Appendix 1 Risk Scorecard Risk Owners and Managers must use the following score card as a guide to accessing the impact and Likelihood of any identified risk;.

Effect	Risk Category	Impacts *Please note* *When drafting a risk description always describe the cause and effect i.e If… then …*	Score
Negligible (1% - 20%)	Financial	Risk (<£50K Capital) or (Revenue <£25K p.a.) Define the value and period, in relation to revenue.	1
	Employee	Low morale is contained within team and managed.	
	Capacity	Short term capacity issue not affecting service delivery.	
	VFM	Negligible impact on value for money. (Revenue <£25K p.a.)	
	H&S wellbeing	Risk to personal health & safety and general wellbeing.	
	Business continuity	Brief interruption of service provision.	
	Contractual Governance	Minor breakdown of shared services or contracts.	
	Reputation	Negligible media coverage/minor complaints.	
	Customer satisfaction	Minimal impact on delivery customer needs.	
	Governance	Poor governance/Internal/ control but zero impact on outcomes.	
	Performance	Targets are missed with no impact on objectives/outcomes.	
	Risks specific to delivery of Corporate Strategy		
	Environmental outcome	Negligible impact on our environmental outcome - Cheltenham's environmental quality and heritage is protected, maintained and enhanced	
	Economic outcome	Negligible impact on our economic outcome - Sustain and grow Cheltenham's economic and cultural vitality	
	Community outcome	Negligible impact on our community economy - People live in strong, safe and healthy communities	
	Business transformation outcome	Negligible impact on our business transformation outcome - Transform our council so it can continue to enable delivery our outcomes for Cheltenham and its residents	
	Risk Category	**Impacts**	
Low (20% - 40%)	Finance	Risk (£50K to £200K Capital) or (Revenue £25K to £50K p.a.) Define the value and period, in relation to revenue.	2
	Employee	Some hostility from staff and minor non-cooperation.	
	Capacity	Short term capacity issue affecting service provision (define term with risk description).	
	VFM	Low impact on value for money. (Revenue £25K to £50K p.a.)	
	H&S and wellbeing	Risk to personal health & safety may result in broken bones and short term illnesses.	
	Business Continuity	Slightly reduced service provision with marginal disruption.	
	Contractual Governance	Some breakdown or shared services or contracts with disruption.	
	Reputation	Adverse local media/negative local opinion/formal complaints.	
	Customer satisfaction	Some customer needs or expectations may not be met either in time or quality.	
	Governance	Governance/Internal/ control has been missed/misunderstood/not up to date resulting in poor decision making.	
	Performance	Targets are missed with low impact on objectives/outcomes.	
	Risks specific to delivery of Corporate Strategy		
	Environmental outcome	Low impact on our environmental outcome - Cheltenham's environmental quality and heritage is protected, maintained and enhanced	
	Economic outcome	Low impact on our economic outcome - Sustain and grow Cheltenham's economic and cultural vitality	
	Community outcome	Low impact on our community economy - People live in strong, safe and healthy communities	
	Business transformation outcome	Low impact on our business transformation outcome - Transform our council so it can continue to enable delivery our outcomes for Cheltenham and its residents	

	Risk Category	Impacts	
Moderate (40% - 60%)	Finance	Risk (£200K to £1M Capital) or (Revenue £50K to £200K p.a.) Define the value and period, in relation to revenue.	3
	Employee	Industrial action in the short term/staff leaving.	
	Capacity	Medium term capacity issues affecting service (define term within risk description).	
	VFM	Moderate impact on value for money. (Revenue £50K to £200K p.a.)	
	H&S and wellbeing	Risk to personal health & safety includes sustained or major illness of 1 or more people.	
	Business Continuity	Services suspended in short term with noticeable disruption.	
	Contractual Governance	Collapse of at least one aspect of shared service or contract with moderate disruption or temporary suspended service.	
	Reputation	Adverse local & media/members questioned.	
	Customer satisfaction	Key customer needs or expectations may not be met either in time or quality.	
	Governance	Governance/Internal/ control arrangements failed leading to non-compliance with legislation and policy.	
	Performance	Targets are missed with impact on objectives/outcomes.	
	Risks specific to delivery of Corporate Strategy		
	Environmental outcome	Moderate impact on our environmental outcome - Cheltenham's environmental quality and heritage is protected, maintained and enhanced	
	Economic outcome	Moderate impact on our economic outcome - Sustain and grow Cheltenham's economic and cultural vitality	
	Community outcome	Moderate impact on our community economy - People live in strong, safe and healthy communities	
	Business transformation outcome	Moderate impact on our business transformation outcome - Transform our council so it can continue to enable delivery our outcomes for Cheltenham and its residents	
	Risk Category	**Impacts**	
Major (60% - 80%)	Finance	Risk (>£1M to £2M Capital) or (Revenue £200K to £500K p.a.) Define the value and period, in relation to revenue.	4
	Employee	Prolonged industrial action/significant number of staff leaving.	
	Capacity	Long term capacity issue affecting service delivery/reputation.	
	VFM	Major failure to provide value for money with major risk and external investigation. (Revenue £200K to £500K p.a.)	
	H&S and wellbeing	Risk to personal health & safety include loss of life/large scale illness.	
	Business Continuity	Service delivery suspended/Priority 1 and Priority 2 ICT systems suspended for long term with major disruption.	
	Contractual Governance	Shared service or contract delivery fails with major disruption.	
	Reputation	Major media coverage. High level of concern from elected members/officers/public with senior staff position threatened.	
	Customer satisfaction	Customer needs or expectations are not met with significant failing in service delivery.	
	Governance	Governance arrangements have failed with major reputation/legal implication and cost to recover.	
	Performance	Targets missed continuously major impact on objectives/outcomes.	
	Risks specific to delivery of Corporate Strategy		
	Environmental outcome	Major impact on our environmental outcome - Cheltenham's environmental quality and heritage is protected, maintained and enhanced	
	Economic outcome	Major impact on our economic outcome - Sustain and grow Cheltenham's economic and cultural vitality	
	Community outcome	Major impact on our community economy - People live in strong, safe and healthy communities	
	Business transformation outcome	Major impact on our business transformation outcome - Transform our council so it can continue to enable delivery our outcomes for Cheltenham and its residents	

	Risk Category	Impacts	
Critical (80% - 100%)	Finance	Risk (>£2M Capital) or (>Revenue £500K p.a.) The value and period, in relation to revenue	5
	Employee	Prolonged industrial action/permanent loss of jobs resulting in inability to deliver services.	
	Capacity	Long term capacity putting at risk personnel, assets, reputation and service delivery.	
	VFM	Critical failure to provide value for money with risk of external investigation and intervention. (>Revenue £500K p.a.)	
	H&S and wellbeing	Risk to personal health & safety includes possibility of multiple fatalities or serious injuries and illness.	
	Business Continuity	Total loss of services, ICT systems and other key assets.	
	Contractual Governance	Shared service and contract delivery fails, resulting in total loss of service or the decommissioning of delivery model.	
	Reputation	Significant local/national media coverage with failure to meet regulatory standard resulting in loss/fine.	
	Customer satisfaction	Customer needs or expectations are not met because of complete failure in service delivery.	
	Governance	Governance/Internal/ control arrangements failed with reputation/legal/cost implication.	
	Performance	If there was a critical failure to deliver on delivery of objectives/outcomes or external investigation and intervention	
	Risks specific to delivery of Corporate Strategy		
	Environmental outcome	A Critical impact on our ability to deliver our environmental outcome - Cheltenham's environmental quality and heritage is protected, maintained and enhanced	
	Economic outcome	A Critical impact on our ability to deliver our economic outcome - Sustain and grow Cheltenham's economic and cultural vitality	
	Community outcome	A Critical impact on our ability to deliver our community economy - People live in strong, safe and healthy communities	
	Business transformation outcome	A Critical impact on our ability to deliver our business transformation outcome - Transform our council so it can continue to enable delivery our outcomes for Cheltenham and its residents	

Likelihood scorecard

Probability	Likelihood Description	Likelihood
0% - 5%	Minimal	1
5% - 15%	Very low	2
15% - 30%	Low	3
30% - 60%	Significant	4
60% - 90%	High	5
> 90%	Very high	6

The total risk score is the multiplication of impact and likelihood when the risk score has been defined consideration must be given as to the best way to manage it, the following table should be used as a guide.

Code	*Risk score*	*Risk Management view*
Red	25 - 30	Must be managed by SLT to reduce risk scores as soon as possible, or agree a contingency plan
Red	16 – 24	Must be managed down to reduce risk scores as soon as possible, or agree a contingency plan and escalated to SLT for consideration
Amber	7 – 15	Seek to improve the risk score in the short/medium term or develop a contingency plan
Green	1 – 6	Tolerate and monitor within the division

Further information

This policy and process document, the full impact scorecard and registers are all available via the Intranet.

CHELTENHAM
BOROUGH COUNCIL

Risk Management Awareness

CBC on-line learning

Updated April 2015

I wonder…

- What is a risk?
- Do we record risks?
- Do we have a policy and process?
- Why do we bother about risk management?
- Who identifies risks?
- Who decides how to manage them?
- Who monitors them?
- What do I have to know and do?

The objective of this module is to give you the answers to these questions.

The outcome is that you will know what *you* need to do about risks and their management.

What is a risk?

An uncertain event or set of events which, should it occur, will have an effect upon the achievement of objectives, within the lifetime of the objective.

What is risk management?

The activities required to identify and control exposure to uncertainty which may impact on the achievement of objectives.

What's CBC's approach to risks?

The council is not risk averse, we believe that risks should be identified and then managed. This means weighing up each risk and taking appropriate action to minimise the impact on our objectives.

Risk management policy

As you might have guessed we do have a policy that governs how we identify and deal with risks at the council.

This module will outline the main points of the policy, but you can read the whole thing here.

Why bother managing risks?

Risk management is sound business practise.

Risk management helps us:

* deliver our objectives and outcomes
* deliver improvements to services
* maintain a safe and healthy environment for the public and our employees
* avoid costly mistakes and insurance claims

Managing risks impacts all of us!

It applies to CBC's stated objectives at all levels: corporate; divisional; service team; project; programme; and individual

So, what has all this got to do with me?

Managing risks supports us in achieving our aims and ambitions.

At your appraisal, each one of the actions you agree with your manager is linked to one of our corporate aims and ambitions.

What should I do?

If you spot a risk that may prevent you achieving one of your actions, bring it to the attention of your line manager, or project manager.

The risk can be assessed and recorded appropriately as it may impact the delivery of your service plan and ultimately the corporate and community strategies.

In a nutshell, employees are responsible for …..

Executive Director	• Promoting the desired culture essential for effective risk management within the council and strategic partners • Assessing and managing corporate risks, including shared services and partnerships
Director	• Assessing and managing corporate and service risks, including shared services and partnerships • Maintaining divisional risk register • Reviewing register quarterly, as a minimum
Service manager	• Documenting risks to achieving team actions in the service risk register • Reviewing risks at management meeting
Employee	• Reporting risks to the delivery of your personal actions to your service manager
Project & programme manager	• Assessing project/programme risks • Documenting risks in project's/programme's risk register
Committee report author	• Including a risk assessment where decisions are required
Corporate governance group	• Reviewing the risk management policy • Reviewing the corporate risk register template and reporting procedure

In a nutshell, Members are responsible for…..

Cabinet and council	• considering any risks associated with the decisions they are asked to make
Cabinet	• considering risk when setting policy • monitoring the risk management process within their respective portfolios
Audit committee	• approving the risk management policy • monitoring appropriate management of risks, via internal audit • annually consider the risk register and make recommendations to Cabinet
Overview and scrutiny committee	• monitoring corporate risk register, as required
Elected Members	• promoting the desired culture essential for effective risk management

How we identify risks?

We operate in a world of change where both internal and external events can pose threats to the achievement of our objectives.
Here are some examples:

Internal sources of risk

- Sufficient finances
- Sufficient skilled, motivated employees
- Appropriate premises
- Technology
- Procurement
- Legal/contractual
- Partners
- Changing priorities
- Accurate information

External sources of risk

- Political change
- Economic change
- Social change
- Environmental change
- Government restructuring
- Customer needs
- Reviews and assessments
- Partnerships, shared services, outsourced services

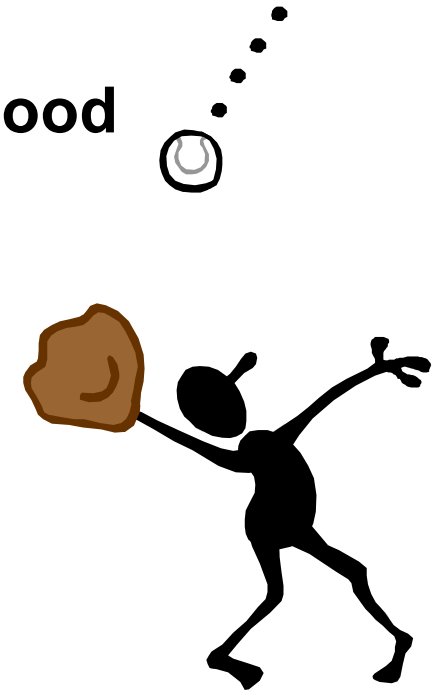
To identify risks we must:

- consider these sources, forward think and anticipate changes
- assess the likelihood of the change occurring
- assess the potential impact on our objectives

How do we assess risks?

Well, we have two criteria for assessing risks, these are:

Likelihood



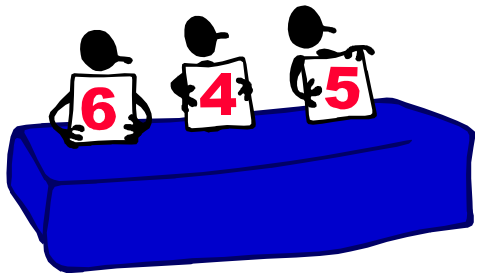
AND

Impact

The two criteria are scored, using CBC's risk scorecard.

Risk scorecard

Take a look at the scorecard



The table gives the guidelines scoring both **Likelihood** and **Impact**.

It provides a framework to allow risks to be defined in a consistent way.

Likelihood and **Impact** scores are multiplied together to obtain the total risk score.

Likelihood is scored on a scale from 1 to 6 - where 1 is almost impossible and 6 is very high.

Impact is scored on a scale from 1 to 5 - where 1 is negligible and 5 is critical.

Risk register

A risk register captures the original risk, it's score and the actions proposed to control the risk.

Once the actions have been implemented the risk is rescored and the risk owner records how any residual risk will be controlled.

CBC risk registers

We have:

- corporate risk register
- service or divisional risk registers
- project and programme risk registers

Take a look at our risk register template.

Tolerance

The risk score indicates it's tolerance level, which in turn shows how the risk should be managed.

Code	*Risk score*	*Risk Management view*
Red	25 - 30	Must be managed by SLT to reduce risk scores as soon as possible, or agree a contingency plan
Red	16 – 24	Must be managed down to reduce risk scores as soon as possible, or agree a contingency plan and escalated to SLT for consideration
Amber	7 – 15	Seek to improve the risk score in the short/medium term or develop a contingency plan
Green	1 – 6	Tolerate and monitor within the division

Responsibility

Each risk has an 'owner'.

It is the risk owner's job to record, action and monitor the risk.

What to do about risks - control

CBC has four options for risk control

- Reduce the risk
  - action that aims to decrease the impact, likelihood, or both
- Accept the risk
  - limited or no action, nothing worth while can be done
- Transfer the risk to a third party
  - action and evaluate the residual risk
- Close the risk
  - there is no longer a potential impact
  - the risk has happened and any residual risk should be treated as a new risk

The risk owner and/or senior officer must identify what action to take in relation to the risk.

The risk, it's score, tolerance and control action is entered into a risk register.

So when do we talk about risks

- 1-2-1s
- Team meetings
- Management team meetings
- Project progress meetings
- Programme board meetings
- Senior leadership team meetings
- Executive board meetings

So do I need to talk about risks?

Now, what do you know about risk management?

This last section is a question and answer session designed to evaluate your understanding of this topic.

The pass mark is 90%.

If you achieve this you can complete this module and print a certificate, if not you will be directed to review the module again.

When answering the questions that follow, please select all answers that apply

Questions

Please read the following questions and select one or more answers to review your understanding of risk management.

1. What is a risk?

1. Any issue
2. Something which may effect the achievement of an action and/or objective
3. Anything that fits with ‘resources, time, quality or outcome’

2. What is risk management?

1. Activity we don’t need to do at CBC
2. Activities to identify and control exposure to uncertainty which may impact on the achievement of objectives
3. Activities to avoid the achievement of objectives

3. Why is risk management important?

1. It helps deliver our objectives and outcomes
2. it helps improve our services
3. It helps maintain a safe and healthy environment for the public and our employees
4. It helps avoid difficult decisions
5. It helps avoid costly mistakes and insurance claims

4. Poor risk management can lead to

1. Bad press, complaints and poor reputation
2. Poor value for money, high costs, wasted time and resources
3. Reduced quality of service delivery

5. Who identifies risks?

1. Any employee
2. Only Executive board
3. Only Service managers

6. We record risks at CBC in…

1. Our heads
2. Risk registers
3. The risk management policy

Questions

Please read the following questions and select one or more answers to review your understanding of risk management.

5. Where can you find the Risk Management Policy?

a) S Drive
b) T Drive
c) Corporate Risk page of the Intranet

6. A risk is scored using a single criteria

1. True
2. False

7. What criteria are used for scoring risks

1. Financial cost
2. Impact
3. Number of people effected
4. Likelihood

8. Who is responsible for reviewing risks?

a) Managers
b) Risk owner and manager
c) Members

9. CBC has a number of risk registers, please tick them

1. corporate risk register
2. SLT risk register
3. service risk registers
4. project and programme risk registers
5. CBC risk register

10. How many options do we have for controlling risks?

1. One
2. Six
3. Four
4. As many as we want

Cheltenham Borough Council

Audit Committee – 23 March 2016

Revised Code of Corporate Governance

Accountable member	**Councillor Steve Jordan - Leader of the Council**
Accountable officer	**Mark Sheldon - Director of Resources**
Ward(s) affected	**None**
Significant Decision	**Yes**
Executive summary	The Council has a Code of Corporate Governance (the Code) that is based upon a SOLACE and CIPFA model; there is a requirement to review it on a regular basis to ensure that it remains up to date and relevant then approved by Members. This year the review was undertaken by the Corporate Governance Group.
Recommendations	I recommend that: Audit Committee consider the Code, suggest any further changes that they feel are appropriate and approve for use during 2016-17.

Financial implications	No direct financial implications *Contact officer: Paul Jones Head of Financial Email: Tel: Paul Jones@cheltenham.gov.uk* *Tel: 01242 775154*
Legal implications	No direct legal implications arising from the recommendations. Contact officer: Peter Lewis Head of Legal Services Email; peter.lewis@tewkesbury.gov.uk Tel; 01684 272012
HR implications (including learning and organisational development)	Cheltenham Borough Council is a partner of the 2020 Joint Committee and a number of former functions of the Council are now the responsibility of the Joint Committee. It is therefore key that changes to the Code are cascaded to all retained and shared services employees working on behalf of Cheltenham Borough Council The Governance arrangements for the Joint Committee and for the council need to dovetail and complement one another. Contact officer: Julie McCarthy HR Manager *Email;, Julie.mccarthy@cheltenham.gov.uk Tel 01242 264355*

Key risks	If the code of Corporate Governance is not kept up to date then there is a risk that we will not meet policy and legislative requirements. If the Council does not maintain a robust governance framework then there is an increased risk to it not doing the right things, in the right way, for the right people, in a timely, inclusive, open, honest and accountable manner. If the Council does not have an effective governance framework then there is an increased risk of error, fraud and corruption. A risk template is attached at appendix 1.
Corporate and community plan Implications	***Effective corporate governance supports the Councils Corporate Strategy, MTFS and partnership working arrangements.***
Environmental and climate change implications	**None**

1. Background

1.1 The current Code was approved by the Audit Committee March 2014, this report informs the Audit Committee of revisions/amendment's and asks members to make further consideration so that any additional suggestions can be included. The draft Code is included at appendix 2.

Role of the Code of Corporate Governance

1.2 The Code is a public statement setting out the governance standards the Council will meet to ensure it is doing the right things, in the right way and operating in an inclusive, open, honest and accountable manner. It provides the organisation and internal and external auditors with assurance that the Council's governance standards are fit for purpose and up to date.

1.3 The Code sets out the Council's standards relating to internal audit, financial control, responding to external audit recommendations, recommendations from formal inspections, and maintaining the internal control environment. The Code also refers to the Constitution and the role of Audit Committee and other committees in providing democratic oversight of the Council's governance arrangements.

1.4 Local authorities are required under the Accounts and Audit (England) Regulations 2011 to prepare an Annual Governance Statement. CIPFA, the Chartered Institute of Public Finance and Accountancy, have produced a local framework entitled 'Delivering Good Governance in Local Government' which recommends both that local authorities produce and maintain a local code of governance and that their annual governance statement reports on the extent to which the code has been complied with. The Council's Code of Corporate Governance is based on the six core principles of the framework, these being:

- Principle 1 - Focusing on the purpose of the Council and on outcomes for the community including citizens and service users and creating and implementing a vision for the local area.
- Principle 2 - Members and officers working together to achieve a common purpose with clearly defined functions and roles.
- Principle 3 - Promoting the values of the Council and demonstrating the values of good governance through behaviour.

- Principle 4 - Taking informed and transparent decisions which are subject to effective scrutiny and managing risk.
- Principle 5 - Developing the capacity and capability of Members and officers to be effective.
- Principle 6 – Engaging with local people and other stakeholders to ensure robust public accountability.

1.5 The Code of Corporate Governance was reviewed by the Corporate Governance Group on the 18 February 2016. The Code has been revised to reflect the comments from the Corporate Governance Group and it is attached as appendix 2 to this report.

Reviewing the Code of Corporate Governance

1.6 CIPFA urges local authorities to ensure their Code of Corporate Governance remains up to date. Since the last refresh of the Code the local government landscape has shifted considerably leading to many new governance issues, for which it is important that the organisation sets out its standards. These include the provisions of the Localism Act 2011, the government's data transparency agenda and the growing awareness of the importance of protecting information.

1.7 In December 2012 CIPFA published a new guidance note for Local Authorities on delivering good governance. The note draws attention to new governance issues, describes how their governance framework should be adhered to following the changes to local government, and includes examples of good governance practices amongst local authorities in responding to these issues. The Code of Corporate Governance takes these issues into account.

1.8 The document refers to a number of track changes to the Council's controls in a number of governance areas which have arisen since the publication of the last Code.

2. Reasons for recommendations

2.1 The Code of Corporate Governance should be up to date and as relevant as possible with the approval of Members.

3. Alternative options considered

3.1 None

4. Consultation and feedback

4.1 Consultation was undertaken with One Legal, members of the Senior Leadership Team and the Corporate Governance group.

5. Performance management –monitoring and review

5.1 The Corporate Governance will review and update the Code as required and report back to Audit Committee on an annual basis.

Report author	**Corporate Governance, Risk and compliance officer** **Contact officer; bryan.parsons@cheltenham.gov.uk,** **01242 264189**

Appendices	1. Risk Assessment 2. Draft Code of Corporate Governance 2016-17
Background information	n/a

Risk Assessment **Appendix 1**

The risk				Original risk score (impact x likelihood)			Managing risk				
Risk ref.	Risk description	Risk Owner	Date raised	Impact 1-5	Likeli-hood 1-6	Score	Control	Action	Deadline	Responsible officer	Transferred to risk register
	If the code of Corporate Governance is not updated and implemented then there is a risk that we will not meet policy and legislative requirements.	Director of Corporate Resources and Projects	23/03/2016	3	1	3	Reduce	Directors to ensure that any key internal Policies are maintained and used in line with the constitution, Financial Rules and Legislation.	01/04/2016	Corporate Governance, Risk and Compliance officer	No
	If the council does not maintain a robust governance framework then there is an increased risk to it not doing the right things, in the right way, for the right people, in a timely, inclusive, open, honest and accountable manner.	Director of Corporate Resources and Projects	23/03/2016	3	1	3	Reduce	Review and revise Code of Corporate Governance	01/04/2016	Corporate Governance, Risk and Compliance officer	No
	If the council does not have an	Director of Corporate	23/03/2016	3	1	3	Reduce	Revise assurance	01/04/2016	Corporate Governance,	No

	effective Governance framework then there is an increased risk of error, fraud and corruption.	**Resources and Projects**						**check lists to measure changes introduced through amendments to the constitution and report within the 2012/13 annual governance statement**		**Risk and Compliance officer**	

Explanatory notes

Impact – an assessment of the impact if the risk occurs on a scale of 1-5 (1 being least impact and 5 being major or critical)

Likelihood – how likely is it that the risk will occur on a scale of 1-6

(1 being almost impossible, 2 is very low, 3 is low, 4 significant, 5 high and 6 a very high probability)

Control - Either: Reduce / Accept / Transfer to 3rd party / Close

CHELTENHAM
BOROUGH COUNCIL

Code of Corporate Governance

Audit Committee Approved Version
April 2016

1. Introduction

What do we mean by Governance?

Governance is about how we ensure that we are doing the right things, in an open, honest and accountable manner.

Good governance comprises the systems, processes, cultures and values we follow so that we can pursue our vision and objectives effectively, while minimising the risks involved. At Cheltenham, we aim to meet the standards of the best and ensure that our governance arrangements are sound.

Good Governance runs through every level of the organisation, it must be owned by all stakeholders, including senior management and members. It forms the essential core values of the Council and should remain embedded in the culture of the council.

Delivering Good Governance

Good governance is important to all officers and members of this Council. It is a key responsibility of our Leader, our Head of Paid Service, the Cabinet, the Senior Leadership Team Council and, in particular the Audit Committee who are responsible for monitoring and providing assurance on our governance arrangements.

The council has in place a process of continual review of its internal control arrangements. The Principles of Good Governance are embedded into the Constitution of the Council, Good Corporate Governance underpins credibility and confidence in the Council and this Code of Corporate Governance promotes accountability, effectiveness, openness, integrity and inclusivity in all of our business.

This Code, the systems that support it and the overall Corporate Governance arrangements are all subjected to an annual audit inspection by the Councils external auditors.

This Local Code also provides a mechanism for the continued development of Corporate Governance arrangements, summarising the principles and how this Council will comply with the Corporate Governance Framework, with Risk Management and with Performance Management.

Testing Our Arrangements

We test our arrangements by:

- Annually reviewing the local code of governance.
- Regular review of our existing governance arrangements against this code.
- Preparing an annual governance statement in order to report publicly on compliance with this code, over the past year.
- Reporting any planned governance changes in the coming period.

In order to review our current arrangements, we:

- Collect assurance statements from Directors on compliance with policies, systems, processes.
- Ensure management and reporting arrangements are in place to monitor governance effectiveness.
- Identify the issues that have not been addressed adequately and consider how they should be addressed.
- Prepare a Significant Issues Action Plan to address issues.
- Ensure appropriate risk and performance management arrangements are in place and are operating effectively.
- Ensure systems of control are working effectively through challenge by Internal Audit.

Background

The Principles of Conduct
There are seven Principles of Public Life which form an important part of the Governance Framework for Members, Officers and partners.

The principles of conduct are:-

- **Selflessness:** Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.
- **Integrity:** Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties.
- **Objectivity:** In carrying out public business, including making public appointments, awarding contracts, or recommending individuals for rewards and benefits, holders of public office should make choices on merit.
- **Accountability:** Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

- **Openness:** Holders of public office should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and actions and restrict information only when the wider public interest clearly demands.
- **Honesty:** Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.
- **Leadership:** Holders of public office should promote and support these principles by leadership and example.

Cheltenham Borough Council's Member Code of Conduct

This Council's Code of Conduct incorporates the principles outlined above and also covers:

- General principles in relation to behaviour and equal treatment of people.
- Confidentiality and openness - the treatment of confidential information and access to information
- Criminal offences and bringing the authority into serious disrepute.
- The prohibition of members from using their office/position to obtain advantage or from using local authority resources for the benefit of political parties.
- Compliance with key policies.
- Decision making - the requirement for members to act reasonably.
- Disclosable Pecuniary Interest - restrictions on participation in meetings by members with an interest in matters under consideration.
- The registration of members' interest - and gifts and/or hospitality received.
- Other significant interest.

Code of Conduct for all employees

Every employee has to acknowledge that they have read and understood this Code of Conduct which incorporates the principles outlined above and also covers:

- Corruption
- Criminal Charges, Convictions and Misconduct
- Reporting Breaches of the Code and Whistleblowing
- Line manager responsibilities,
- All employees have to make an annual declaration of Interest to meet the requirements of section 117 of the Local Government Act.

How do we use the Core Governance Principles to maintain our Code of Corporate Governance?

Development of the Principles of Governance

In 2007 the CIPFA/SOLACE joint working group issued a framework based upon six Core Governance principles this was called Delivering good Governance in Local Government. This was aimed at helping Local Authorities develop and maintain their own codes of governance.

Those six core governance principles are to:-

1. focus on the purpose of the authority and on outcomes for the community and creating and implementing a vision for the local area;
2. ensure that Members and Officers work together to achieve a common purpose with clearly defined functions and roles;
3. promote the values of good governance through upholding high standards of conduct and behaviour;
4. take informed and transparent decisions which are subject to effective scrutiny and managing risk;
5. develop the capacity and capability of members and officers to be effective; and
6. engage with local people and other stakeholders to ensure robust public accountability.

Core Governance Principles

The Council can demonstrate how it complies with these six core principles through a range of specific policies, guidance and internal controls.

2. Compliance with the Six Principles

Principle 1 - Focusing on the purpose of the Council and on outcomes for the community and creating and implementing a vision for the local area

To support the requirements of this principle the Council is committed to undertaking the following:-

In order to exercise strategic leadership the Council will:-	**This will be achieved through:-**
• Develop and promote the authority's vision, ambition, key priorities and values. • Review on a regular basis the authority's vision, ambition for the local area and its impact on the authority's governance arrangements. • Ensure that partnerships are underpinned by a common vision of their work that is understood and agreed by all parties. • Publish an annual report on a timely basis to communicate the authority's activities and achievements, its financial position and performance.	➢ Identify review and communicate the authority's vision by consulting with elected Members service users and citizens ➢ Corporate Strategy and annual action plan ➢ People Strategy ➢ Annual Performance Report ➢ Cheltenham Partnership annual action plan
In order to ensure users receive quality services whether directly, in partnership or by commissioning the Council will:-	**This will be achieved through:-**
• Decide how the quality of service for users is to be measured and make sure that the information needed to review service quality effectively and regularly is available. • Put in place effective arrangements to identify and deal with failure in service delivery.	➢ Corporate Strategy and annual action plan ➢ Commissioning Protocol ➢ Annual Performance Report and quarterly updates to SLT ➢ Appropriate governance frameworks i.e. Limited company, trust or mutual ➢ Effective client management arrangements
In order to ensure the Council makes best use of resources and that taxpayers and service users receive excellent value for money the Council will:-	**This will be achieved through:-**

• Decide how value for money is to be measured and make sure that the authority or any partnership arrangements which the authority has made, has the information needed to review value for money and performance effectively. • Measure the environmental impact of policies, plans and decisions.	➢ Undertake budget consultation exercises ➢ Procurement Strategy ➢ Medium Term Financial Plan ➢ Corporate strategy objectives ➢ Analysing complaints against its decisions

Principle 2 - Members and officers working together to achieve a common purpose with clearly defined functions and roles

To support the requirements of this principle the Council is committed to undertaking the following:-

In order to ensure effective leadership throughout the organisation the Council will: -	**This will be achieved through:-**
• Set out a clear statement of the respective roles and responsibilities of Members both in terms of committee and individual responsibilities and the authority's approach towards putting this into practice. • Set out a clear statement of the respective roles and responsibilities of senior officers. • Establish clear roles and responsibilities for the Scrutiny Committee.	➢ Local Code of Conduct for Members and Co-opted Members ➢ Code of Conduct for Officers ➢ Constitution ➢ Terms of reference for Committee ➢ Terms of reference for the Inter-authority agreement/Shared Service Partnerships ➢ Protocol for Member/Officer Relations ➢ People Strategy ➢ Commissioning Protocol ➢ Job specifications and descriptions ➢ Effective and relevant training

In order to ensure a constructive working relationship exists between members and officers the Council will: -	This will be achieved through:-
• Determine a scheme of delegation and reserve powers within the constitution, including a formal schedule of those matters specifically reserved for collective decision within the authority taking account of relevant legislation and ensure that it is monitored and updated when required. • Make the Head of Paid Service responsible and accountable to the authority for operational management in the role as Head of Paid Service. • Develop protocols to ensure that the Leader and Head of paid Service negotiate their respective roles early in the relationship and that a shared understanding of roles and objectives is maintained. • Make the Section 151 Officer responsible to the authority for ensuring that appropriate advice is given on all financial matters, for keeping proper financial records and accounts, and for maintaining an effective system of internal financial control. • Make the Monitoring Officer responsible to the authority for ensuring lawfulness and fairness of decision making.	➢ Member/Officer Protocol ➢ Scheme of Delegation to Officers ➢ Constitution ➢ Terms of reference for the Head of Paid Service ➢ Defined functions for the Section 151 Officer ➢ Constitution and Financial regulations ➢ Defined Functions for Monitoring Officer in Constitution
In order to ensure its relationships with its partners and the public are clear, the Council will:-	**This will be achieved through:-**
• Develop protocols to ensure effective communication between members and officers in their respective roles. • Set out the terms and conditions for remuneration of members and officers and an effective structure for managing the process, including an effective job evaluation process for officers' remuneration and a remuneration panel for members. • Ensure that effective mechanisms exist to monitor service delivery. • Ensure that its ambition, strategic plans, priorities and targets are developed through robust mechanisms, and in consultation with the local community and other key stakeholders, and that they are clearly articulated and disseminated. • When working in partnership ensure that members are clear about their roles and responsibilities, both individually and collectively, in relation to the	➢ Member/Officer Protocol ➢ Members Allowances Scheme ➢ Terms and Conditions of Employment for employees ➢ Pay and grading framework ➢ Performance Appraisal process for employees ➢ Disciplinary and Grievance Procedures ➢ Performance Management Framework ➢ Consultation Strategy ➢ Development Plan ➢ Debt Management Policy

partnership and to the authority.	➢ HB/CTB Overpayments policy
• When working in partnership: - ensure that there is clarity about the legal status of the partnership - ensure that representatives or organisations both understand and make clear to all other partners the extent of their authority to bind their organisation to partner decisions.	➢ Commissioning Protocol ➢ Commissioning toolkit ➢ Legal agreements between each party

Principle 3 - Promoting values for the Council and demonstrating the values of good governance through upholding high standards of conduct and behaviour

To support the requirements of this principle the Council is committed to undertaking the following:-

In order to ensure members and officers exemplify good standards of conduct the Council will:-	
• Ensure that the authority's leadership sets a tone for the organisation by creating a climate of openness, support and respect • Ensure that standards of conduct and personal behaviour expected of members and staff, of work between members and staff and between the authority, its partners and the community are defined and communicated through codes of conduct and protocols • Put in place arrangements to ensure that members and staff are not influenced by prejudice, bias or conflicts of interest in dealing with different stakeholders and put in place appropriate processes to ensure that they continue to operate in practice	➢ Counter-Fraud and Corruption Strategy ➢ Whistle-Blowing Policy ➢ Staff Satisfaction Surveys ➢ Local Code of Conduct for Members ➢ Code of Conduct for all employees ➢ Register of Member Interests and Gifts and Hospitality ➢ Declaration of Members interests ➢ Registers of Officers Interests ➢ Register of Gifts, Hospitality and Sponsorship

	➢ Equality Policy ➢ Safeguarding policy Handbook
In order to ensure organisational values are put into practice the Council will:-	
• Develop and maintain, articulate and communicate corporate and leadership values both for the organisation and staff, reflecting public expectations and communicate these with members, staff, the community and partners. • Put in place arrangements to ensure that procedures and operations are designed in conformity with appropriate ethical standards, and monitor their continuing effectiveness in practice. • Develop and maintain an effective standards committee.	➢ Corporate values ➢ 5 year Corporate Plan ➢ Annual Action Plan ➢ Constitution ➢ Terms of Reference of the Standards Committee ➢ People Strategy ➢ Organisational competencies
• Use its corporate values to act as a guide for decision making and as a basis for developing positive and trusting relationships within the authority. • In pursuing the vision of a partnership, agree a set of values against which decision making and actions can be judged. Such values must be demonstrated by partners' behaviour both individually and collectively.	➢ Corporate values ➢ Commissioning Protocol

Principle 4 - Taking informed and transparent decisions which are subject to effective scrutiny and managing risk

To support the requirements of this principle the Council is committed to undertaking the following:-

In being rigorous and transparent about how decisions are taken the Council will:-	**This will be achieved through:-**

• Develop and maintain an effective scrutiny function which encourages constructive challenge and enhances the Council's performance overall and the performance of any organisation which it scrutinises • Develop and maintain open and effective mechanisms for documenting evidence for decisions and recording the criteria, rationale and considerations on which decisions are based • Put in place arrangements to safeguard members and staff against conflicts of interest and put in place appropriate processes to ensure that they continue to operate in practice. • Put in place effective transparent and accessible arrangements for dealing with complaints	➢ Overview and Scrutiny Procedure Rules ➢ Agendas and Minutes ➢ Access to Information Procedure Rules ➢ Guidance on decision making and recording of decisions ➢ Registers of Member Interests and Gifts and Hospitality ➢ Register of Officer decisions ➢ Registers of Officers Interests ➢ Register of Gifts, Hospitality and Sponsorship ➢ Complaints Procedures ➢ Freedom of Information ➢ Publication scheme ➢ Transparency Policy ➢ Terms of Committee Reference ➢ Promotion of Openness and Honesty Culture
In order to ensure the Council has good quality information, advice and support to ensure that services are delivered effectively and are what the community wants/needs it will:-	**This will be achieved through:-**
• Ensure that those making decisions whether for the authority or a partnership are provided with information that is fit for the purpose, relevant, timely and gives clear explanations of technical issues and their implications. • Ensure that professional advice on matters that have legal or financial implications is available and recorded well in advance of decision making and used appropriately	➢ Committee reporting guidelines ➢ Consultation with finance, HR and legal built into report template
In order to ensure there is an effective system of risk management the Council will:-	**This will be achieved through:-**

• Ensure that risk management is embedded into the culture of the organisation, with members and managers at all levels recognising that risk management is part of their job • Ensure that arrangements are in place for whistle blowing to which staff and all those contracting with the authority have access.	➢ Risk Management Policy ➢ Business Continuity Strategy ➢ Counter-Fraud and Corruption Strategy ➢ Whistle-Blowing Policy ➢ Promotion of Openness and Honesty Culture
In order to use its legal powers for the full benefit of the community the Council will:-	**This will be achieved through:-**
• Actively recognise the limits of lawful activity placed on them by, for example the ultra vires doctrine but also strive to utilise powers to the full benefit of their communities. • Recognise the limits of lawful action and observe both the specific requirements of legislation and the general responsibilities placed on local authorities by public law. • Observe all specific legislative requirements placed upon them, as well as the requirements of general law, and in particular to integrate the key principles of good administrative law – rationality, legality and natural justice into its procedures and decision making processes.	➢ Constitution ➢ Corporate Strategy and annual action plan ➢ Medium Term Financial Strategy ➢ Defined roles and responsibilities for the Head of Paid Service ➢ Defined roles and responsibilities for the section 151 officer ➢ Defined roles and responsibilities for the Monitoring Officer

Principle 5 - Developing the capacity and capability of members and officers to be effective

To support the requirements of this principle the Council is committed to undertaking the following:-

In order to make sure members and officers have the necessary skills and resources the Council will:-	**This will be achieved through:-**
• Provide induction programmes tailored to individual needs and opportunities for members and officers to update their knowledge on a regular basis.	➢ Members induction and training programme ➢ Corporate Appraisal scheme

• Ensure that the statutory officers have the skills, resources and support necessary to perform effectively in their roles and that these roles are properly understood throughout the organisation.	➢ Personal Development Plans ➢ Annual Budget
In order to develop the capability of people with governance responsibilities the Council will:-	**This will be achieved through:-**
• Assess the skills required by members and officers and make a commitment to develop those skills to enable roles to be carried out effectively • Develop skills on a continuing basis to improve performance including the ability to scrutinise and challenge and to recognise when outside expert advice is needed • Ensure that effective arrangements are in place for reviewing the performance of the authority as a whole and agreeing an action plan which might for example aim to address any training or development needs	➢ Commissioning Protocol ➢ Members induction and training programme ➢ Self assessments of committee effectiveness ➢ Annual Performance Report and quarterly updates to SLT ➢ Prince project methodology includes performance review ➢ Lessons learnt exercises carried out following significant projects
In order to encourage new members of the authority the Council will:-	**This will be achieved through:-**
• Ensure that effective arrangements designed to encourage individuals from all sections of the community to engage with, contribute to and participate in the work of the authority. • Ensure that support is in place for members and officers to encourage participation and development.	➢ The Cheltenham Partnership ➢ Elected Members development plan ➢ Briefing Seminars

Principle 6 - Engaging with local people and other stakeholders to ensure robust public accountability

To support the requirements of this principle the Council is committed to undertaking the following:-

In order to exercise leadership through a robust scrutiny function the Council will:-	**This will be achieved through:-**
• Make clear to all stakeholders and the community to whom it is accountable and for what. • Consider those institutional stakeholders to whom it is accountable and assess the effectiveness of the relationships and any changes required. • Produce an annual report on scrutiny function activity.	➢ Constitution ➢ Complaints Procedures ➢ Freedom of Information requests ➢ Counter Fraud, Corruption and Bribery Policy ➢ Whistle-Blowing Policy ➢ External and Internal Audit reports ➢ Commissioning Protocol
In order to take an active approach to dialogue with accountability to the community, it will ensure effective and appropriate service delivery either directly by the Council, in partnership or through commissioning by:-	**This will be achieved through:-**
• Ensuring that clear channels of communication are in place with all sections of the community and other stakeholders including monitoring arrangements to ensure that they operate effectively. • Holding meetings in public unless there are good reasons for confidentiality. • Ensuring arrangements are in place to enable the authority to engage with all sections of the community effectively. These arrangements should recognise that different sections of the community have different priorities and establish explicit processes for dealing with these competing demands. • Establishing a clear policy on the types of issues it will meaningfully consult on or engage with the public and service users, including a feedback mechanism for those consultees to demonstrate what has changed as a result. • Publishing an annual report giving information on the authority's ambition, strategy, plans and financial statements as well as information about its outcomes, achievements and the satisfaction of service users in the previous	➢ Customer Services Strategy ➢ Access to Information Procedure Rules (FOI) ➢ Equality and Diversity ➢ Commissioning Protocol ➢ Annual Performance Report and quarterly updates to SLT ➢ ICT Strategy

period. • Ensuring that the authority as a whole is open and accessible to the community, service users and its staff and ensure that it has made a commitment to openness and transparency in all its dealings, including partnerships subject only to the need to preserve confidentiality in those specific circumstances where it is proper and appropriate to do so.	Transparency Policy
In order to make best use of human resources the Council will:-	**This will be achieved through:-**
• Develop and maintain a clear policy on how staff and their representatives are consulted and involved in decision making.	➢ A People Strategy ➢ Policy for consultation on Health and Safety and welfare ➢ Joint consultative committee arrangements ➢ Workforce Change (HR Policies and guidance)

3. Monitoring compliance with the framework

The Corporate Governance Group will, in line with its terms of reference consider and monitor on a regular basis any issues placed on its significant issues action plan (SIAP) to strengthen the Council's governance arrangements. Progress against the SIAP will be monitored by the Corporate Governance Group and reported to the Senior Leadership Team and the Audit Committee, which will assist in the completion of the Annual Governance Statement.

4. Annual Assurance Assessment

Although the review of the corporate governance arrangements will be an ongoing process, each year the Directors will be required to sign an Annual Governance Certificate assessing the effectiveness of their divisions corporate governance arrangements, the results of which will form the basis of the Annual Governance Statement.

The Annual Governance Statement will be agreed by the Audit Committee and then included in the Annual Report and Statement of Accounts to be agreed by full council.

The Annual Governance Statement will be informed by, and based upon the work undertaken by the Corporate Governance Group which is chaired by the Chief Executive, and attended by other senior officers including the Section 151 Officer, the Monitoring Officer and the Head of Internal Audit.

Cheltenham Borough Council

Audit Committee – 23 March 2016

Review policy guidelines and new policy and procedures for the Acquisition of Communications Data using The Regulation of Investigatory Powers Act 2000 (RIPA)

Accountable member	**Cabinet Member Corporate Services, Councillor Walklett**
Accountable officer	**Director Resources, Mark Sheldon**
Ward(s) affected	**None**
Key Decision	**n/a**
Executive summary	**Existing policy review** To brief Audit Committee on the Regulation of Investigatory Powers Act (RIPA) 2000 and to request that members consider the Councils own RIPA Procedural Guidance document. The Cheltenham Borough Council (CBC) RIPA Procedural Guidance summarises the duties and responsibilities based upon the Codes of Practice and will be used by all officers involved in this activity. There have been no substantive changes to this policy since last year but it has been brought up to date to reflect the new senior management structure and the roles and responsibilities of the officers involved in the authorisation/management of the RIPA process. **New Policy** A new Policy and Procedures Document for the Acquisition of Communications Data using The Regulation of Investigatory Powers Act 2000 (RIPA) has been drafted to provide transparency and guidance on the process. A local authority must be a paid up member of National Anti-Fraud Network (NAFN) in order to make use of its single point of contact (SPoC) service in relation to communications data. The Council is a member, primarily to make use of other services provided by NAFN (credit referencing, DVLA checks, debtor tracing etc.) but given that officers could now utilise the RIPA SPoC service and obtain communications data, legislative guidance needs to be in place to govern the process. RIPA and this new policy controls the obtaining of communications data by authorised employees. This data does not include the content of the communications i.e. the actual email message, letter, text or telephone conversation merely details basic subscriber information and the frequency of communication. A local authority may only acquire communications data for the purpose of the prevention or detection of crime or the prevention of disorder.
Recommendations	1. To consider and make recommendations in respect of the existing CBC RIPA Procedural Guidance (appendix 2); and to approve its continued use 2. To approve the new Policy and Procedures Document for the acquisition of Communications Data using The Regulation of

Investigatory Powers Act 2000 (RIPA) (appendix 3)

Financial implications	There are no financial implications arising from this report. **Contact officer: Sarah Didcote, Sarah.Didcote@Cheltenham.gov.uk, 01242 264125**
Legal implications	This report ensures that the Council complies with the guidance issued by the Home Office to support the Statutory Code of Practice in ensuring member oversight of the use of the Council's surveillance powers. The Council may where it is necessary and proportionate need to undertake surveillance. RIPA provides a legal framework for the control and regulation of surveillance and information techniques which public authorities undertake as part of their duties. The Council's procedural guide will provide information and advice to those seeking authorisation and those officers granting authorisation. It will also provide the public with information about how the Council approaches using the surveillance. Judicial Approval will be required before an Authorisation is granted in respect of surveillance. The Proper Officer for Authorisation is the Chief Executive (pg423), Executive Director (pg424), Director of Resources (pg425) and Director of Built Environment (pg426) **Contact officer: Donna C Marks, donna.marks@tewkesbury.gov.uk , 01684272068**
HR implications (including learning and organisational development)	Regular training sessions will be provided to ensure that staff are fully conversant with The Regulation of Investigatory Powers Act 200 (RIPA). **Contact officer: Carmel Togher, HR Business Partner, carmel.togher@cheltenham.gov.uk, 01242 775215**
Key risks	*If surveillance or the obtaining of communications data is carried out without due regard to RIPA, Ministry of Justice Codes of Practice and the CBC procedural guidance then there are risks to an individual's rights and to the Council's reputation.*
Corporate and community plan Implications	None
Environmental and climate change implications	None

1. Background - Existing policy review

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) is the law concerning the use of covert techniques by public authorities.

1.2 It requires that when public authorities need to use covert techniques to obtain private information about someone, they do it in a way that is necessary, proportionate and compatible with human rights.

1.3 Members will be aware from previous reports in respect of the Council's use of RIPA powers, that it must have in place a system of authorising, recording and reviewing any surveillance that it carries out that is covered by the Act.

2. RIPA Authorisations

2.1 The Council is included within the RIPA framework with regard to the authorisation of both directed surveillance and of the use of Covert Human Intelligence Sources (CHIS). The Council is only able to authorise surveillance under RIPA if it is for the purpose of preventing, or detecting crime or preventing disorder subject to the "serious offence test". Before giving authorisation an authorising officer must be satisfied that the reason for the request is for the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. one of the permitted reasons under the Act and permitted under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 i.e.

- the desired result of the covert surveillance cannot reasonably be achieved by other means;
- the risks of collateral intrusion have been properly considered, whether the reason for the surveillance is balanced proportionately against the risk of collateral intrusion;
- there must also be consideration given to the possibility of collecting confidential personal information. If there is a possibility of collecting personal information the matter should be passed to the chief officer for consideration.

3. Revised RIPA Policy Guidelines

3.1 A copy of the revised CBC RIPA Guidance is attached at Appendix 2. The changes take account of the new management structure. They also include guidance to officers in relation to:

Internet Investigations

3.2 The use of the internet as an investigative method is now becoming routine. However, just because the information being obtained is from the internet, staff must still consider all the normal rules and guidance applicable to any type of enquiry conducted within a criminal investigation, such as, the Data Protection Act (DPA), Criminal Procedures Investigations Act (CPIA) and RIPA. In the Surveillance Codes of Practice issued December 2014 there is a section dealing with these types of enquiries.

Reporting errors

3.3 There is a requirement to report all covert activity that was not properly authorised to the OSC in writing as soon as the error is recognised. This would be known as an error. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer.

Surveillance outside of RIPA

3.4 Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) mean that a local authority can now only grant an authorisation under RIPA where the local authority is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

3.5 As a result of the changes in legislation, it is envisaged that surveillance may be required which falls outside of RIPA (for example in the case of anti-social behaviour offences which do not attract a maximum custodial sentence of at least six months imprisonment). This guidance covers that eventuality.

Equipment

3.6 All equipment capable of being used for Directed Surveillance such as cameras etc. should be approved for that purpose by the authorising officer.

Joint Agency Surveillance

3.7 In cases where one agency is acting on behalf of another, it is usual for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

4. New Policy - Acquisition of Communications Data using The Regulation of Investigatory Powers Act 2000 (RIPA)

4.1 The Council has a procedural guide for the use of RIPA which has been in place for some time and it should be noted that this document does not replace it. Any officer considering the use of RIPA as part of an investigation should follow the original guidance in the first instance.

4.2 Since September 2014, local authorities can only access communications data via the National Anti-Fraud Network (NAFN):

4.3 The Council is a member of NAFN, primarily to make use of other services provided by them (credit referencing, DVLA checks, debtor tracing etc.) but given that officers could now utilise the RIPA Single Point of Contact (SPoC) service and obtain communications data, guidance needs to be in place to govern the process.

4.4 This procedural guide is based on the requirements of The Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office Code of Practice on the Acquisition and Disclosure of Communication Data.

4.5 If any of the Home Office Codes of Practice change, the appropriate guide will be updated, and the amended version placed on the internet / published accordingly. Regular training sessions will also be provided to ensure that staff members are fully conversant with the Act.

4.6 Part 1 Chapter 2 of RIPA controls the obtaining of communications data by Local Authority staff. This data does not include the content of the communications i.e. the actual email message, letter, text or telephone conversation.

4.7 Part 1 also introduces a statutory framework to regulate access to communications data by public bodies consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in these processes. In addition it puts safeguards in place to balance the rights of the individual against the needs of society, as a whole, to be protected from crime and other public safety risks. This thus reflects the requirements of Article 8 of the European Convention on Human Rights; the right to privacy.

4.8 This policy reflects the requirements of the legislation and the Home office Interception of Communications Code of Practice issued January 2016

Communications data available to local authorities

4.9 The types of information that we are allowed to access fall into two categories and detailed with paragraph 3.1 of the policy:

1. Subscriber Information (RIPA S21(4)(c)) - Information about Communications Services Users:

2. Service Use Data (RIPA S 22(4)(b) - Information about the use of Communications

Services:

The Council is not allowed to access:

4.10 The Council cannot access certain communication data this is detailed within section 3.2 of the policy; traffic data.

Power to obtain communications data

4.11 There are two powers granted by S22 RIPA in respect of the acquisition of communications data from telecommunications and postal companies or 'Communications Service Providers'

4.12 1. A notice under S22(4). and

4.13 2. An authorisation under S22(3).

4.14 These two powers are detailed within section 4 of the policy.

Procedure for Obtaining Communications Data

4.15 There is now only one method that officers can use to obtain communications data; by way of the NAFN secure website. To use this system applicants have to individually register on the NAFN website. A Designated Person will also need to be registered to authorise the applicant's requests. Further information on this procedure is covered within section 5 of the policy and additional guidance can be provided by the Internal Audit Department.

Roles and responsibilities

4.16 The policy provides for the roles and responsibilities of those involved in the process. The Senior Responsible Officer is accountable for the following:

- The integrity of the processes of acquiring communications data;
- Compliance with the act and code of practice;
- Oversight of the reporting of errors to IOCCO;
- Engaging with IOCCO inspectors when they conduct inspections;
- Overseeing the implementation of any post-inspection action plans.

4.17 The Head of Paid Service is the Senior Responsible Officer with regard to the acquiring of communications data.

Central Records

The Council must retain copies of all applications, authorisations, copies of notices and withdrawals of authorisations and cancellation of notices, cross-referenced against each associated document. This will be coordinated by the RIPA Coordination Officer who also holds copies of application for actual surveillance as per the Council's overarching RIPA policy.

Interception of Communications Commissioner's Office

4.18 The exercise of the powers and duties relating to communications data is kept under review by inspectors who work for the Interception of Communications Commissioner's Office (IOCCO) under the control of the Interception of Communications Commissioner.

4.19 IOCCO state that if we receive a Freedom of Information request for a copy of our inspection report we should notify IOCCO, who will provide us with a suitably redacted version of the report to submit to the requester. No disclosure must take place until IOCCO has been consulted.

Strategy and Policy Review

4.20 The Internal Audit Department will review and amend this policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the vision of the Council.

5. Reasons for recommendations

5.1 It is essential that these powers are used for the proper purpose and in the correct way; these policies and guidance will ensure that that happens and that elected members are kept fully informed.

5.2 If authorisation is given for the use of surveillance using RIPA then a briefing informing the Audit Committee of what action has been taken will be made as soon as possible and where appropriate. It should be noted that the Council use these powers very sparingly and only when there is no other alternative.

6. Alternative options considered

6.1 None

7. Consultation and feedback

7.1 The Corporate Governance Group, Audit Cotswold and officers involved in investigation and surveillance activities work have been consulted. Advice has also been sought from One Legal.

8. Performance management – monitoring and review

8.1 There will be reports to the Audit Committee on the use of RIPA.

Report author	**Contact officer: Bryan Parsons** **Email: bryan.parsons@cheltenham.gov.uk Tel: 01242 264189**
Appendices	1. Risk Assessment 2. RIPA guidance

Risk Assessment **Appendix 1**

The risk				Original risk score (impact x likelihood)			Managing risk				
Risk ref.	Risk description	Risk Owner	Date raised	Impact 1-5	Likeli-hood 1-6	Score	Control	Action	Deadline	Responsible officer	Transferred to risk register
	If surveillance is carried out without due regard to RIPA, Codes of Practice and the CBC procedural guidance then there are risks to an individual's rights and to the Councils reputation.	Head of paid Service	23/03/2016	4	2	8	Accept	• Put in place effective management and guidance. • Promote the guidance with Service managers and investigation staff.	Ongoing	Head of Internal Audit	
	If the Council fails to put in place adequate policy and process covering the use of RIPA powers in resect of the aquision and interception of communication data then there is a risk that the	Head of paid Service	23/03/2016	4	2	8	Accept	• Put in place effective management and guidance. Promote the guidance with Service managers and investigation staff.	Ongoing	Head of Internal Audit	

	Counciols reputation and assets are put at risk.										

Explanatory notes

Impact – an assessment of the impact if the risk occurs on a scale of 1-5 (1 being least impact and 5 being major or critical)

Likelihood – how likely is it that the risk will occur on a scale of 1-6

(1 being almost impossible, 2 is very low, 3 is low, 4 significant, 5 high and 6 a very high probability)

Control - Either: Reduce / Accept / Transfer to 3rd party / Close

Regulation of Investigatory Powers Act (RIPA) Procedural Guide

(Including additional guidance on Non - RIPA surveillance)

Document History
Document Location S: Library drive

Control Location: Code of Corporate Governance

Review Period: Annual

Reviewed by: Corporate Governance Group

Version Number	Version Date	Summary of Changes
1.0	**16/04/2013**	**Revised Guidance**
1.1	**March 2015**	**Revised by Audit Comm**
1.2	**March 2016**	**Revised by Audit Comm**

This document is owned by:

Name	Job Title	Version
Mark Sheldon	Director Resources	1.1

This document has been distributed to:

Name	Job Title	Version
All CBC employees, Members, and on the Public website		1.0

Index

Forward:

This revised guidance reflects two significant legislative changes.

1. **Approval of RIPA Authorisations by a Justice of the Peace:** The amendments in the Protection of Freedoms Act 2012 mean that the authorisations and notices under RIPA for the use of particular covert techniques can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).

2. **Directed surveillance crime threshold:** Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 means that we can only grant an authorisation under RIPA for the use of directed surveillance when investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

This guidance provides advice on how Cheltenham Borough Council can best approach these changes in law and the new arrangements that need to be put in place to implement them effectively. It is supplementary to the legislation and to the statutory Codes of Practice. If there any doubts about the guidance then the RIPA coordinator or One Legal should be consulted.

This guidance is intended for investigation officers that may use covert techniques, including Environmental Health, Benefit Fraud Officers and Enforcement Officers. However, it will also be of use to authorising officers and designated persons and to those who oversee the use of investigatory techniques including elected members.

Surveillance outside of RIPA
There may be a necessity for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation such as in cases of serious disciplinary investigations or for overt operations this guidance provides some advice on the process for those situations.

The Council must still meet its obligations under the Human Rights Act and any surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and the management of such surveillance must be well documented.

There is also a requirement for the Council's Senior Responsible Officer (SRO) to regularly monitor surveillance outside of RIPA. Therefore before any such surveillance takes place advice must be sought from Legal Services. Guidance is contained within this policy for this type of surveillance.

The Human Rights Act means that the Council by law has to respect the rights of everyone. In particular Article 8 guarantees everyone the right to respect for their private and family life, their home and correspondence. This right can only be interfered with when the interference is in accordance with the law and necessary. RIPA provides the framework for public authorities to carry out surveillance and the lawful means whereby rights can be infringed by the Council.

Cheltenham Borough Council undertakes to use these powers in line with the law, only when necessary and proportionately.

Steve Jordan. Leader.
Cheltenham Borough Council

1 INTRODUCTION

1.1 RIPA presents some difficult judgments which must be made from time to time. Whilst individual services can and do operate their own procedures, this is an issue which affects the Council corporately and staff will never be criticised for seeking advice.

1.2 The first point to emphasise is that any person who is unsure about whether to seek authorisation or unsure about whether to issue an authorisation, must seek immediate advice before acting. For those seeking authorisation, advice may initially be sought from their line manager, but it is always appropriate to seek the advice of a member of One Legal. RIPA is a piece of legislation with serious human rights implications whenever it is engaged. The Council is concerned about an individual's rights, but it is also concerned to guard against serious reputational risk.

1.3 The purpose of this document is to ensure that the Council complies with the Regulation of Investigatory Powers Act 2000 (RIPA).

1.4 This document provides guidance on the regulation of any covert surveillance that is carried out by council officers. This includes the use of undercover officers, informants and private investigators and other agents of the Council.

1.5 Any covert surveillance will have to be authorised and conducted in accordance with RIPA, the statutory codes of practice (issued in December 2014) and this Guide and shall only be for one of the purposes set out in this Guide and for a purpose which the Council is legally required or empowered to investigate as part of its functions.

1.6 Covert surveillance will only be used by the Council where it judges such use to be necessary and proportionate to the seriousness of the crime or matter being investigated,

1.7 Before requesting authorisation Investigating Officers will have regard to this document and the statutory Codes of practice issued under section 71 RIPA (current version issued in December 2014). The Codes of practice are available from the RIPA Co-ordinator and direct from the Office of Surveillance website at http://www.surveillancecommissioners.gov.uk/ or the Home Office at http://security.homeoffice.gov.uk/ripa/.

1.8 Before authorising covert surveillance Authorising Officers will have regard to this Guide and the statutory Codes of Practice. The Codes of Practice are available from the Home Office, CBC RIPA Co-ordinator and direct from the Office of Surveillance website or the Home Office.

1.9 Authorising Officers will have to consider whether it is necessary and proportionate for Investigating Officers to undertake covert surveillance and whether it is possible to obtain the evidence through other means. The role of the authorising officer is covered in greater detail within paragraph 4.2 of this doicument.

1.10 Authorising Officers must give detailed consideration to the risk of collateral intrusion i.e. the risk of intruding into the privacy of others while watching someone else. This consideration and how the intrusion should be reduced and managed will need to be recorded within the application form.

1.11 There must be no situation where a council officer engages in covert surveillance without obtaining authorisation in accordance with the procedures set out in this document, the statutory Codes of Practice and from RIPA.

1.12 Any queries concerning the content of the document should be addressed to the RIPA Co-ordinator (Governance, Risk and Compliance officer CBC).

2 THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA)

2.1 The background to RIPA

RIPA provides a legal framework for the control and regulation of surveillance and information techniques which public authorities undertake as part of their duties. As was highlighted in the introduction to the Guide the need for such control arose as a result of the Human Rights Act 1998. Article 8 of the European Convention on Human Rights states that:-

1) Everyone has the right of respect for his private and family life, his home and his correspondence.

2) There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.

2.1.1 The right under Article 8 is a qualified right and authorities can interfere with this right for the reasons given in paragraph 2 of Article 8. RIPA provides the legal framework for lawful interference.

2.2 The scope of this Guide

2.2.1 This Guide intends to cover the surveillance and information gathering techniques which are most likely to be carried out by the Council.

2.2.2 Neither RIPA nor this Guide covers the use of any overt surveillance, general observation that forms part of the normal day to day duties of officers, the use of equipment to merely reinforce normal sensory perception such as binoculars or circumstances where members of the public who volunteer information to the Council.

2.2.3 RIPA does not normally cover the use of overt CCTV surveillance systems since members of the public are aware that such systems are in place.

2.2.4 There may however be times when the Council uses CCTV for a specific investigation or operation. This Guide does not cover in detail the use of surveillance via the Town Centre CCTV system. In such cases authorisation for directed surveillance may be required. If the CCTV is to be used for surveillance, Investigating Officers should consult and adhere to the provisions of RIPA and the Cheltenham Town Centre Closed Circuit Television Operating Procedures and the Cheltenham Town Centre Closed Circuit Television Codes of practice jointly set up by Cheltenham Borough Council and Gloucestershire Constabulary.

2.2.5 If an Investigating Officer envisages using any other CCTV system they should contact the RIPA Co-ordinator concerning any clarification on the administrative process or seek legal advice from One Legal before they conduct any surveillance.

2.3 Consequences of not following RIPA

2.3.1 Section 27 of RIPA provides that surveillance shall be lawful for all purposes if authorised and conducted in accordance with an authorisation granted under RIPA.

2.3.2 Lawful surveillance is exempted from civil liability.

2.3.3 Although not obtaining authorisation does not make the authorisation unlawful per se, it does have some consequences: -

i. Evidence that is gathered may be inadmissible in court;

ii. The subjects of surveillance can bring their own proceedings or defeat proceedings brought by the Council against them on human rights grounds i.e. we have infringed their rights under Article 8;

iii. If a challenge under Article 8 is successful the Council could face a claim for financial compensation;

iv. A complaint could be made to the Office of Surveillance Commissioners; and

v. The Government has also introduced a system of tribunal. Any person who believes that their rights have been breached can have their complaint dealt with by way of a tribunal.

2.4 The Surveillance Commissioner

2.4.1 The Government has appointed a Surveillance Commissioner to review the way in which public authorities implement the requirements of RIPA. The Commissioner has a wide range of powers of access and investigation. The Council will receive periodic visits from the Office of the Surveillance Commissioners. They will check to see if the Council is complying with RIPA.

2.4.2 It is important that the Council can show it complies with this Guide and with the provisions of RIPA.

3 COVERT SURVEILLANCE

There are three categories of covert surveillance: -

1. Directed Surveillance;
2. Covert Human Intelligence Sources; and
3. Intrusive surveillance (Local Authorities are not permitted to carry out intrusive surveillance). The information is included in this procedural guide to avoid inadvertent use of intrusive surveillance. Intrusive surveillance is defined in RIPA as surveillance in respect of anything taking place on residential premises or in a private vehicle, involving the presence of an investigator on those premises/vehicles or carried out through a surveillance device.

3.1 Directed Surveillance (DS)

3.1.2 The majority of covert surveillance that will be undertaken by the Council will fall under the heading of Directed Surveillance (DS).

3.1.3 DS is defined as surveillance which is covert, but not intrusive, and is undertaken:

a) For the purpose of a specific investigation or operation

b) In such a manner as it is likely to result in obtaining private information about a person (whether or not that person is the target of the investigation or operation) and

c) In a planned manner and not by way of an immediate response, whereby it would not be reasonably practicable to obtain an authorisation prior to the surveillance being carried out.

3.1.4 Any car park where Automated Number Plate Recognition (ANPR) is installed for either payment or enforcement purposes or it is intended to use that equipment to monitor a particular vehicle or person beyond that purpose then the use of RIPA legislation should be considered.

3.1.5 It is irrelevant where the subject of the DS is being observed.

If you intend to instruct an agent to carry out the DS the agent must complete and sign the form marked "agent's agreement form" contained in Appendix C. The agent will be subject to RIPA in the same way as any employee of the Council would be. They may also be inspected by the OSC in respect of that particular operation. This should be pointed out during the instruction and contract stage. The Authorising Officer should ensure that the agents are qualified or have the necessary skills to achieve the objectives. They should also ensure that they understand their obligations under RIPA. If advice is required please contact One Legal.

3.1.6 The flow chart in Table 1 and 2 provides guidance on the council's procedure for making an application to a Justice of the Peace (JP) seeking an order to approve the grant of a RIPA authorisation or Notice.

3.2 Covert Human Intelligence Sources (CHIS)

This involves the establishment or maintenance of a personal or other relationship with a person for the covert purpose of obtaining or disclosing information. A CHIS is a person who: -

a) S/He establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);

b) S/He covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c) S/He covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

3.2.1 A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

3.2.2 A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

3.2.3 Covert human intelligence sources may only be authorised if the following arrangements are in place:

• that there will at all times be an officer within the council who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security, (the handler) the investigation officer

• that there will at all times be another officer within the council who will have general oversight of the use made of the source; (controller) i.e. the responsible line manager.

• that there will at all times be an officer within the council who has responsibility for maintaining a record of the use made of the source; and

• that the records relating to the source maintained by the council will always contain particulars as laid down by the Covert Human Intelligence Sources codes of practice (current version issued in December 2014)

3.2.4 Legal advice should always be sought where consideration is given to the use of CHIS.

3.2.5 Special consideration must be given to the use of vulnerable individuals for CHIS. A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description, or a juvenile as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive (or, in his absence, the Deputy Chief Executive).

3.2.6 Before you undertake any surveillance involving a vulnerable individual (CHIS) you must consult One Legal before authorisation is sought.

3.2.7 Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him.

3.2.8 In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for juvenile sources should be granted by Chief Officers. Before you undertake any surveillance involving a juvenile you **must** consult the RIPA Co-ordinator concerning any clarification on the administrative process or seek legal advice from One Legal.

3.2.9 If you intend to instruct an agent to be the CHIS, the agent must complete and sign the form marked "agent's agreement form" contained in Appendix C. The agent will be subject to RIPA in the same way as any employee of the Council would be. They may also be inspected by the OSC in respect of that particular operation. This should be pointed out during the instruction and contract stage. If advice is required please contact either the RIPA Co-ordinator or One Legal.

3.2.10 The flow chart in Table 1 below provides guidance on the council's procedure for making an application to a Justice of the Peace seeking an order to approve the grant of a RIPA authorisation or Notice.

Table 2 is a copy of the guidance provided to JP/Magistrate s on the process for dealing with an application from the council.

Appendix E provides additional information about the process the RIPA application and authorisation process by a JP/Magistrate

Table 1:

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE

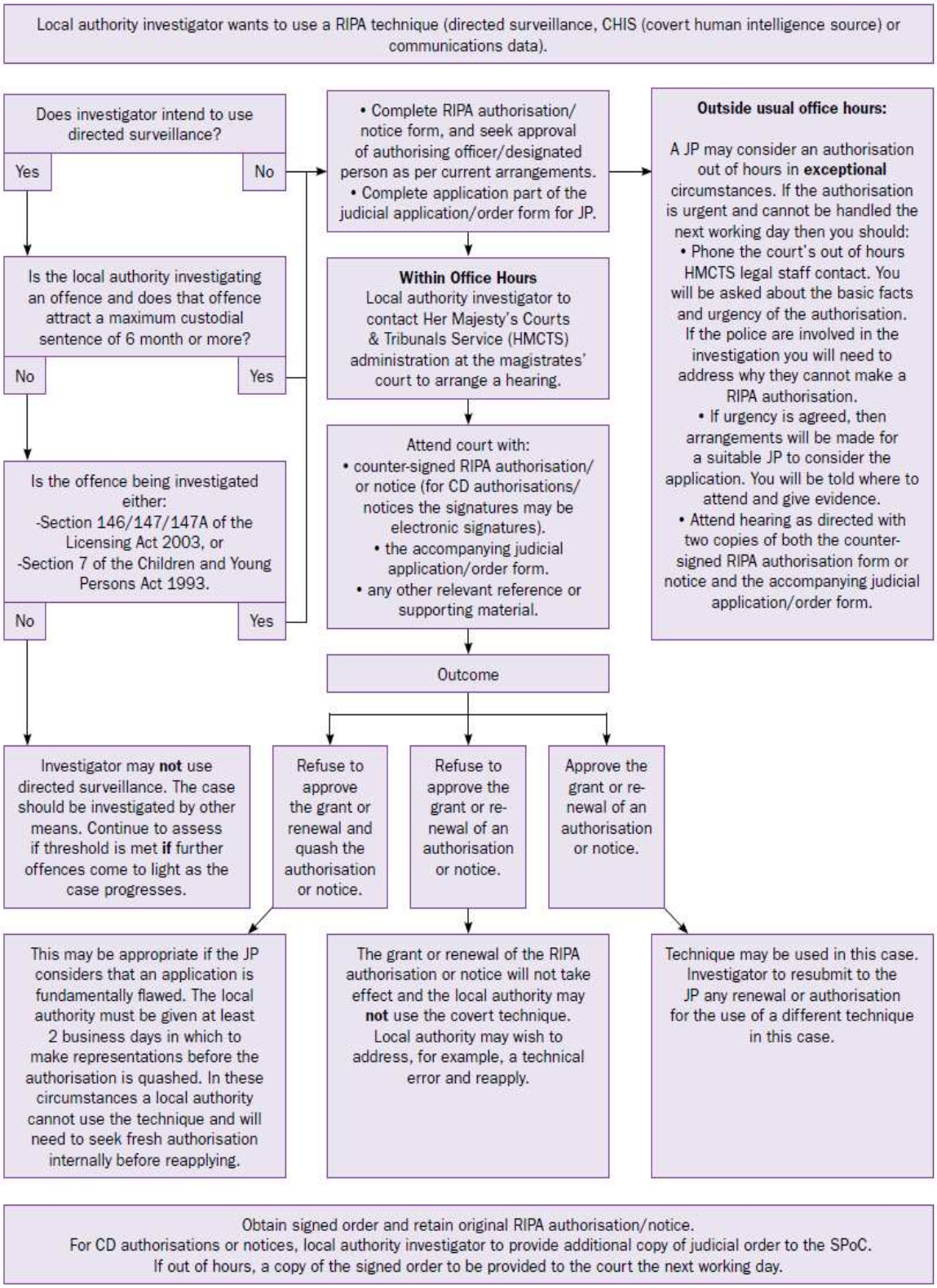


Table 1

PROCEDURE: LOCAL AUTHORITY APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE

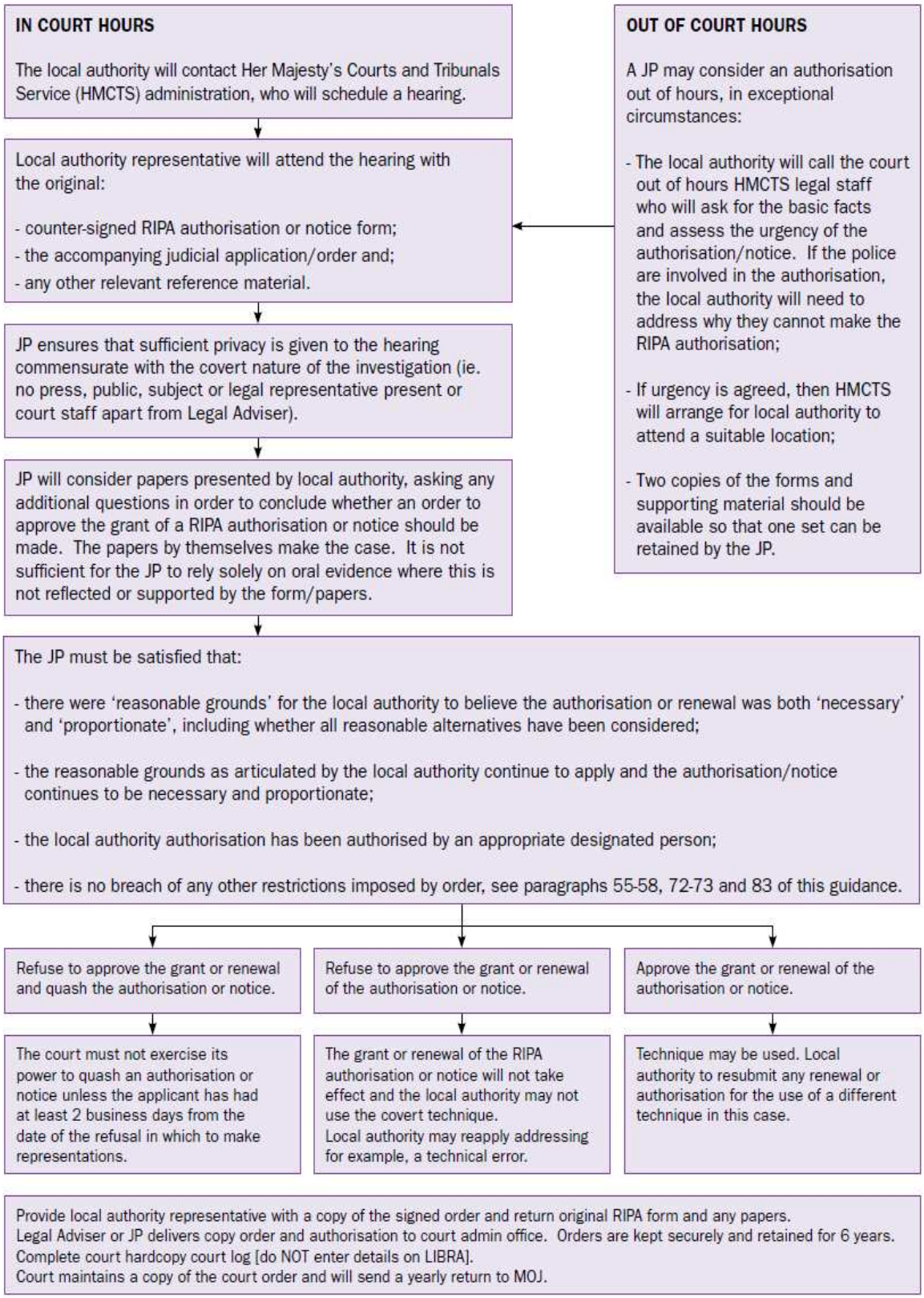


Table 2

3.3 Intrusive surveillance

Intrusive surveillance is defined as covert surveillance that: -

a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

b) involves the presence of any individual on the premises or in the vehicle or is carried out by means of a surveillance device.

c) If the device is not located on the premises or in the vehicle, it is not intrusive surveillance unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Operatives will need to be aware of using high powered zoom lenses or CCTV that may fall into this category.

3.3.1 *Local authorities are not authorised to conduct intrusive surveillance*

3.3.2 If you are considering conducting surveillance and the surveillance might fall within the scope of intrusive surveillance you **must** contact the RIPA Co-ordinator concerning any clarification on the administrative process or seek legal advice from One Legal before you undertake any surveillance.

4 PROCEDURE FOR OBTAINING AUTHORISATIONS

4.1 The Senior Responsible Officer:-

Role:

4.1.1 The nominated Executive Director is the Senior Responsible Officer (SRO) with responsibilities for:

4.1.2 (a) ensuring the integrity of the Council's RIPA processes;

(b) ensuring compliance with RIPA legislation and the Home Office RIPA Codes of practice;

(c) engaging with the OSC when its inspector conducts an inspection;

(d) overseeing the implementation of any post – inspection plans;

(e) ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations made by the OSC inspection reports;

(f) ensuring that concerns are addressed, where OSC inspection reports highlight

(g) concerns about the standards of Authorising Officers.

(h) must regularly monitor covert surveillance activity which takes place outside of RIPA as mentioned in the OSC Procedures and Guidance document.

4.2 Authorising Officers

4.2.1 The role of the Authorising Officers is to authorise, review, renew and cancel directed surveillance.

4.2.2 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. Where an Authorising Officer authorises such an investigation or operation the Central Record of Authorisations should highlight this and it should be brought to the attention of a Commissioner or Inspector during their next inspection.

4.2.3 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for local authorities the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation.

4.2.4 A designated Authorising Officer must qualify **both** by rank and by competence. Officers who wish to be designated must have been trained to an appropriate level so as to have an understanding of the Act and the requirements that must be satisfied before an authorisation can be granted.

Appendix A lists the officers within the Council who can grant authorisations all of which are at Strategic or Director level.

4.2.5 Authorisations must be given in writing by the Authorising Officer. They must complete the relevant section on the application form and explain exactly what they are authorising, against who, in what circumstances, where etc. It is important that this is very clear as the surveillance operatives are only allowed to carry out what is authorised. This will assist with avoiding errors. They must believe the surveillance is **proportionate** to what it seeks to achieve, taking into account the **collateral intrusion** issues, and that the level of the surveillance is appropriate to achieve the objectives.

4.2.6 If any equipment such as covert cameras, video cameras is to be used, the Authorising Officer should know the capability of the equipment before Authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision. They may be required to justify their actions in a court of law or some other tribunal.

4.2.7 Authorising Officers are also responsible for carrying out regular reviews of applications which they have authorised and also for the cancellation of authorisations.

4.2.8 Authorised Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA (current version issued December 2014 and the latest Procedures and Guidance from the Office of Surveillance Commissioner (OSC). This latter document details their latest guidance to be followed and Authorising Officers are required to hold their own copy.

4.3 Authorising Officers – What you need to do before authorising surveillance

4.3.1 Before giving authorisation an Authorising Officer **must** be satisfied that the reason for the request is for the **prevention and detection of crime and that** the crime attracts a custodial sentence of a maximum of 6 months or more (Table 1 page 11), or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. one of the permitted reasons under the Act and permitted under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 i.e.

- the desired result of the covert surveillance cannot reasonably be achieved by other means
- the risks of collateral intrusion have been properly considered, whether the reason for the surveillance is balanced proportionately against the risk of collateral intrusion
- there must also be consideration given to the possibility of collecting confidential personal information. If there is a possibility of collecting personal information the matter should be passed to the Chief Officer for consideration

4.3.2 An Authorising Officer **must** also be satisfied the surveillance in each case is **necessary** and **proportionate in those particular circumstances and demonstrate by completing the relevant section of the authorisation how they reached their decision.**

Nessity and Proportionality are defined as:

Necessity

Obtaining an authorisation under the 2000 Act, the 1997 Act and 1994 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. The 2000 Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds which, for Local Authorities is the **prevention and detection of crime and that** the crime attracts a custodial sentence of a maximum of 6 months or more or for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco The applicant and Authorising Officers must also be able to demonstrate that there were no other means of obtaining the same information in a less intrusive method.

Proportionality

Then, if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.
When explaining proportionality the Authorising Officer should explain why the methods and tactics to be adopted during the surveillance is not disproportionate.

4.3.3 The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

4.3.4 When the Authorising Officer has considered if the surveillance is necessary and proportionate they must complete the relevant section of the form explaining why in his/her opinion the surveillance is necessary and proportionate. They should also detail the exact activity being authorised, who against etc. in the relevant authorisation section on the form.

4.3.5 The applicant will now be required to complete the relevant forms and attend Magistrates' Court to seek a JP's approval (see Appendices D,E or F on the RIPA Application and Authorisation Process)
Appendix G provides the contact details for Her Majesty's Courts and Tribunal Service

4.4 Investigating Officers – What you need to do before applying for authorisation

4.4.1 Investigating Officers should think about the need to undertake DS or CHIS before they seek authorisation. Investigating Officers need to consider whether they can obtain the information by using techniques other than covert surveillance. There is nothing that prevents an Investigating Officer discussing the issue of surveillance beforehand.

4.4.2 Appendix E provides guidance on the full application and authorisation procedure, including the application process to seek approval from a Justice of the Peace. This should be read by all staff.

4.4.3 The applicant or some other person must carry out a feasibility study as this may be required to be seen by the Authorising Officer. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Guide and the statutory Codes of Practice.

4.4.4 The form should then be submitted to the Authorising Officer for authorisation.

5 DURATION, REVIEW, RENEWAL AND CANCELLATION OF AUTHORISATIONS

5.1 Duration

5.1.1 Directed Surveillance (DS) authorisations will cease to have effect after three months from the date of approval by the magistrate unless renewed or cancelled. They do not expire, they must be cancelled when the surveillance is no longer proportionate or necessary.

5.1.2 Authorisations should be given for the maximum duration but reviewed on a regular basis and formally cancelled when no longer needed.

5.1.3 CHIS authorisations will cease to have effect after twelve months from the date of approval.

5.1.4 Investigating Officers should indicate within the application the period of time that they estimate is required to carry the surveillance, this will be proportionate to the objectives of the investigation and give due consideration to collateral intrusion

5.1.5 For CHIS authorisations, legal advice must be sought, particularly those that involve the use of juveniles (for which the duration of such an authorisation is one month instead of twelve months).

5.1.6 It is the responsibility of the Investigating Officer to make sure that the authorisation is still valid when they undertake surveillance.

5.2 Review

5.2.1 An Investigating Officer must carry out a regular review of authorisations. If an authorisation is no longer required or considered to be no longer *necessary* or *proportionate* it **must** be cancelled.

5.2.2 The results of any review must be included on the review form Appendix B

5.2.3 The Authorising Officer also has a duty to review authorisations that have been granted when it is necessary or practicable to do so. Particular attention should be given to authorisations involving collateral intrusion or confidential material.

5.2.4 The Authorising Officer should keep a copy of the review form and a copy should be given to the Investigating Officer. The original copy of the review form must also be sent to the RIPA Co-ordinator.

5.3 Renewals

5.3.1 An Investigating Officer must ask an Authorising Officer to grant a renewal of an authorisation before it would cease to have effect. The approval of a Justice of the Peace (JP) is required prior to undertaking any covert activity as detailed within the renewal form (Appendix B) authorised by the Authorising Officer for a renewal to take affect.

5.3.2 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a JP to consider the application).

5.3.3 Applications for renewal must not be made more than 3 working days before the authorisation is due to expire.

5.3.4 A renewal can last for up to three months, effective from the date that the previous authorisation would ceased to have effect.

5.3.5 An Authorising Officer can grant more than one renewal as long as the request for authorisation still meets the requirements for authorisation. An Authorising Officer must still consider all of the issues that are required for a first application before a renewal can be granted. Each renewal will need the approval of a JP.

5.3.6 If the reason for requiring authorisation has changed from its original purpose it will not be appropriate to treat the application as a renewal. The original authorisation should be cancelled and a new authorisation should be granted.

5.3.7 An application for a renewal must be completed on the appropriate form. Appendix B

5.3.8 The Authorising Officer and applicant should retain a copy of the renewal and the judicial application / order form. A copy of the original renewal form and the judicial application/order form must also be sent to the RIPA Co-ordinator for the Central Register

5.4 Cancellations

5.4.1 If the reason for requiring the authorisation no longer exists, the authorisation **must** be cancelled and in any event as soon as the operation for which an authorisation was sought ceases to be necessary or proportionate. This applies to both original applications and renewals.

5.4.2 Authorisations **must** also be cancelled if the surveillance has been carried out and the original aim has been achieved.

5.4.3 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form Appendix B. The date and time when such an instruction was given should also be recorded in the central record of authorisations.

5.4.4 The Investigating Officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc.

5.4.5 Authorisations **must** also be cancelled if the surveillance has been carried out and the original aim has been achieved. Authorising Officers will ensure that authorisations are either cancelled or renewed at the end of the appropriate statutory period.

5.4.3 An authorisation must be cancelled by using the form in Appendix B. An Investigating Officer should complete the details required on the first page, sections 1 and 2 of the cancellation form. The form should then be submitted to the Authorising Officer who will complete sections 3, 4 and 5.

5.4.4 It is the responsibility of the Investigating and Authorising Officers to monitor their authorisations and cancel them where appropriate.

5.4.5 The Authorising Officer should keep a copy of the cancellation form and a copy should be given to the Investigating Officer. A copy of the original cancellation form must also be sent to the RIPA Co-ordinator.

5.4.6 Authorising Officers must review upon cancellation of an application whether or not the objectives were achieved. Any issues identified by the review will be reported to the senior responsible officer.

5.5 Review of Policy and Procedure

i The Audit Committee will receive reports following the use of RIPA. Those reports will contain information on;

- Where and when the powers had been used
- The objective
- The authorisation process
- The job title of the Authorising Officer
- The outcome including any legal court case
- Any costs

ii The Corporate Governance Group will review any use of RIPA and report to Audit Committee on an annual basis.

6 THE RIPA CO-ORDINATOR

6.1 **Role**

6.1.1 All original applications for authorisations and renewals including those that have been refused must be passed to the RIPA Co-ordinator as soon as possible after their completion with copies retained by the Authorising Officer and the Applicant.

6.1.2 All cancellations must also be passed to the RIPA Co-ordinator.

6.1.3 The RIPA Co-ordinator will: -

i.. Keep the copies of the forms for a period of at least 3 years;

ii.. Keep a register of all of the authorisations, renewals and cancellations; and Issue the unique reference number.

iii.. Keep a database for identifying and monitoring expiry dates and renewal dates.

iv. Along with, Directors, Service Managers, Authorising Officers, and the Investigating Officers must ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Councils Information Management policies, departmental retention schedules and the Data Protection Act 1998. (DPA)

v. Provide administrative support and guidance on the processes involved.

vi. Not provide legal guidance or advice.

vii.. Monitor the authorisations, renewals and cancellations so as to ensure consistency throughout the Council;

viii.. Monitor each department's compliance and act on any cases of non compliance;

ix.. Provide training and further guidance on and awareness of RIPA and the provisions of this Guide; and

x.. Review the contents of the Guide.

6.1.4 It is however the responsibility of the Investigating Officer, the Authorising Officer and the Senior Responsible Officer to ensure that: -

i. Authorisations are only sought and given where appropriate;

ii. Authorisations are only sought and renewed where appropriate;

iii. Authorisations are cancelled where appropriate; and

iv. They act in accordance with the provisions of RIPA.

7.0 Legal advice

i One Legal will provide legal advice to staff making, renewing or cancelling authorisations

ii Requests for legal advice will be in writing and copied to the RIPA Co-ordinator to keep on file

iii Reponses to requests for legal advice will be in writing and copied to the RIPA coordinator to keep on file.

8.0 Internet Investigations

8.1 The use of the internet as an investigative method is now becoming routine. However, just because the information being obtained is from the internet staff must still consider all the normal rules and guidance applicable to any type of enquiry conducted within a criminal investigation, such as, the Data Protection Act (DPA), Criminal Procedures Investigations Act (CPIA) and RIPA. In the Surveillance Codes of Practice issued December 2014 there is now a section dealing with these types of enquiries. The paragraph titled Online Covert Activity within the Codes of Practice is replicated below at 8.2 and should be taken into consideration should staff wish to carry out internet open source enquiries, particularly where Social Networking Sites are involved.

8.2 The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

8.3 If staff wish to conduct internet enquiries, particularly Social Networking Sites they must consider the intrusion issues on the subject of the enquiries and other innocent people (collateral intrusion) and when obtaining the evidence this must be stored in line with the Data Protection Act. They must also consider whether they are monitoring in line with the surveillance definition. If so, and they are likely to obtain private information they are likely to require authorisation under the RIPA legislation. These activities are forming part of the RIPA inspections and will also be audited internally.

9.0 Reporting Errors

9.1 There is no a requirement to report all covert activity that was not properly authorised to the OSC in writing as soon as the error is recognised. This would be known as an error. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply. This will require a report detailing any remedial action taken. The Council also has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Chief Surveillance Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

9.2 This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA. ***Urgent Authorisations***

As from 1 November 2012 there is no provision under RIPA for urgent oral authorisations

10.0 Surveillance Outside of RIPA

10.1 Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that a local authority can now only grant an authorisation under RIPA where the local authority is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

10.2 As a result of the changes in legislation, it is envisaged that surveillance may be required which falls outside of RIPA (for example in the case of anti-social behaviour offences which do not attract a maximum custodial sentence of at least six months imprisonment). The Office of Surveillance Commissioners Procedures and Guidance 2011 states that it is prudent to maintain an auditable record of decisions and actions to use covert surveillance without the protection of RIPA and that such activity should be regularly reviewed by the SRO. The SRO will therefore maintain an oversight of non RIPA surveillance in her role as SRO to ensure that such use is compliant with Human Rights legislation. The RIPA Monitoring Officer will maintain a central record of non RIPA surveillance.

10.3 As part of the new process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form (see appendix H) should be completed and authorised by a service manager. A copy of the non RIPA surveillance application form can be found on the Intranet or is available from the RIPA Monitoring Officer.

10.4 Non RIPA surveillance also includes staff surveillance which falls outside of RIPA. Any surveillance of staff must be formally recorded on the non-RIPA surveillance Application Form and authorised by the Head of Service in consultation with the Head of Internal Audit. A central record of staff surveillance is also maintained by the SRO.

11.0 Equipment

11.1 All equipment capable of being used for Directed Surveillance such as cameras etc. should be for their purpose by the Authorising Officer, fit for purpose for which they are intended. The equipment should be logged on the central register of equipment held by the RIPA Co-Ordinator. This will require a description, Serial Number, an explanation of its capabilities.

11.2 When completing an Authorisation the applicant must provide the Authorising Officer with details of any equipment to be used and its technical capabilities. The Authorising Officer will have to take this into account when considering the intrusion issues and proportionality. The Authorising Officer must make it clear on the Authorisation exactly what equipment if any they are authorising and in what circumstances.

12.0 Joint Agency Surveillance

12.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

12.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application form to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Monitoring Officer. This will assist with oversight of the use of Council staff carrying out these types of operations.

APPENDIX A

Designated Officers

The following officers are the Senior Responsible Officer and the Authorising Officers for the purposes of RIPA

Senior Responsible Officer

Head of Paid Service Pat Pratley

Authorising Officers

Director Resources and Projects ; M Sheldon. Director of Place and Economic Development Tim Atkins.

Where the guidance states the Senior Responsible Officer but they are unavailable then a Director not involved in the authorisation process will undertake the duties of the Senior Responsible Officer.

RIPA Co-ordinator
Corporate Governance, Risk and Compliance Officer. B Parsons

APPENDIX B

AUTHORISATION FORMS

All of the forms necessary for RIPA are available from the Home Office website.

www.gov.uk/government/collections/ripa-forms--2

These forms are a mandatory part of the process and must be used in line with the guidance.

All decisions about using regulated investigatory powers must be recorded as they are taken on the required form.

This is the case for:

- applicants seeking authority to undertake regulated conduct
- Authorising Officers and designated persons who consider and decide whether to grant authority or give notice for that conduct

Select the form that you require from the hyperlinked lists below;

Directed Surveillance

1. Application for the use of directed surveillance
2. Renewal of directed surveillance
3. Review of the use of directed surveillance
4. Cancellation of the use of directed surveillance

Covert Human Intelligence Sources

5. Application for the use of covert human intelligence sources
6. Renewal of authorisation to use covert human intelligence sources
7. Reviewing the use of covert human intelligence sources
8. Cancellation of covert human intelligence sources

Reporting errors to the IOCCO

9. Reporting an error by a CSP to the IOCCO
10. Reporting an error by a public authority to the IOCCO

APPENDIX C

REGULATION OF INVESTIGATORY POWERS ACT 2000

AGENT'S AGREEMENT FORM

I ……(insert Agent's name) of ….. ……(address) confirm that in relation to …… …… …… …… …… …… ……(name or description of the surveillance) I agree to comply with the Regulation of Investigatory Powers Act 2000, with all statutory provisions, statutory Codes of practice and with Cheltenham Borough Council's Procedural Guide when undertaking any and all surveillance authorised by Cheltenham Borough Council under the Regulation of Investigatory Powers Act 2000. I acknowledge receipt of a copy of the Council's Authorisation Form reference number ……..dated the …… and I agree not to carry out any surveillance that is contrary this authorisation.

Signed…….

Dated……..

APPENDIX D

Particulars to be contained in records when a COVERT HUMAN INTELLIGENCE SOURCE (CHIS) is used.

The following matters are specified for the purposes of paragraph (d) of section 29(5) of the 2000 Act (which must be included in the records relating to each CHIS):

(a) the identity of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the authority maintaining the records;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(j) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(k) the information obtained by each relevant investigating authority by the conduct or use of the source;

(l) any dissemination by that authority of information obtained in that way; and

(m) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

In addition, records or copies of the following, as appropriate, should be kept by the relevant authority:

(a) a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;

(b) a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

(c) the reason why the person renewing an authorisation considered it necessary to do so;

(d) any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;

(e) any risk assessment made in relation to the source;

(f) the circumstances in which tasks were given to the source;

(g) the value of the source to the investigating authority;

(h) a record of the results of any reviews of the authorisation;

(i) the reasons, if any, for not renewing an authorisation;

(j) the reasons for cancelling an authorisation.

(k) the date and time when any instruction was given by the Authorising Officer to cease using a source.

The records kept by public authorities should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person within the relevant public authority who will have responsibility for maintaining a record of the use made of the source.

APPENDIX E

RIPA Application and Authorisation Process

As from 1 November 2012 two significant changes came into force that effects how local authorities use RIPA.

- **Approval of Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean that the council's authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that the council can now only grant an authorisation under RIPA for the use of Directed Surveillance where the council is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

- This crime threshold, as mentioned, is only for Directed Surveillance.

Application, Review, Renewal and Cancellation Forms

No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.
The effect of the above legislation means that all applications and renewals for covert RIPA activity will have to have a JP's approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

The procedure is as follows;

All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP's approval.

The applicant will complete the relevant application form ensuring compliance with the statutory provisions shown above. The application form will be submitted to an Authorising Officer for consideration. If authorised, the applicant will also complete the required section of the judicial application/order form (Appendix F)

Although this form requires the applicant to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well. All applications need to be made in consultation with One Legal.

It will then be necessary within Office hours to arrange with Her Majesty's Courts & Tribunals Service (HMCTS) administration at the Magistrates' Court to arrange a hearing. The hearing will be in private and heard by a single JP.

Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP. If in doubt as to whether you are able to present the application seek advice from One Legal

Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case, and the original application/authorisation form.

The original RIPA application/authorisation should be shown to the JP but will be retained by the council so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The JP will read and consider the RIPA application/ authorisation and the judicial application/order form Appendix F. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form**. However the forms and supporting papers must by themselves make the case. It is not sufficient for the council to provide oral evidence where this is not reflected or supported in the papers provided**.

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the council and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The JP may decide to:

Approve the Grant or renewal of an authorisation
The grant or renewal of the RIPA authorisation will then take effect and the council may proceed to use the technique in that particular case.

Refuse to approve the grant or renewal of an authorisation
The RIPA authorisation will not take effect and the council may **not** use the technique in that case.

Where an application has been refused the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the application/authorisation has met the tests, and this is the reason for refusal the officer should consider whether they can reapply, for example, if there was information to support the application which was available to the council, but not included in the papers provided at the hearing.

For, a technical error (as defined by the JP/Magistrate), the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation or notice

This applies where the JP refuses to approve the application/authorisation or renew the application/authorisation and decides to quash the original authorisation or notice. However the court must not exercise its power to quash the application/authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform the One Legal who will consider whether to make any representations.

Whatever the decision the JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the council's RIPA application and authorisation form and the judicial application/order form. The officer will retain the original application/authorisation and a copy of the judicial application/order form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date, the officers are now allowed to undertake the activity.

The original application and the copy of the judicial application/order form should be forwarded to the Central Register and a copy retained by the applicant and if necessary by the Authorising Officer.

The council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, One Legal will decide what action if any should be taken.

All the relevant forms for authorisation through to cancellation must be in writing using the standard forms which are available from the Intranet site, but officers must ensure that the circumstances of each case are accurately recorded on the application form.

If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective applications forms and procedures should be followed and both activities should be considered separately on their own merits.

An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

Applications

All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the activities being undertaken by the staff. The Line Manager will perform an initial quality check of the application. However they should not be involved in the sanctioning of the authorisation. Completed application forms are to be initialed by Line Managers to show that the quality check has been completed. The form should then be submitted to the Authorising Officer.

Applications whether authorised or refused will be issued with a unique number (obtained from the RIPA Coordinator) by the Authorising Officer, taken from the next available number in the Central Record of Authorisations which is held by the RIPA Coordinator.

If authorised the applicant will then complete the relevant section of the judicial application/order form and follow the procedure above by arranging and attending the Magistrates' Court to seek a JP's approval. (See procedure above RIPA application and authorisation process)

Duration of Applications

- Directed Surveillance 3 Months
- Renewal 3 Months
- Covert Human Intelligence Source 12 Months
- Juvenile Sources 1 Month
- Renewal 12 months

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire. (See cancellations page 16)

Reviews

When an application has been authorised regular reviews must be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

The reviews are dealt with internally by submitting the review form (which is available through the link in appendix B) to the Authorising Officer. There is no requirement for a review form to be submitted to a JP.

In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably, or the techniques to be used are now different a new application form should be submitted and will be required to follow the process again and be approved by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Service mangers of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

Renewal

A renewal form is to be completed by the applicant when the original authorisation period is about to expire but directed surveillance is still required

Should it be necessary to renew a Directed Surveillance or CHIS application/authorisation this must be approved by a JP. The renewal forms can be found by following the links in appendix B

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a JP to consider the application).

The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

If the Authorising Officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

The cancellation form Appendix B is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations..

The Investigating Officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

Appendix F

Application for judicial approval for authorisation to obtain or disclose communications data, to use a Covert Human Intelligence Source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....
.....

.....
.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....
.....

.....
.....

.....
.....

.....
.....

.....
.....

.....
.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....
....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant

department:.....

.....
.....

Contact telephone
number:.....

Contact email address
(optional):.....

Local authority
reference:.....
.

Number of
pages:.....
.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates'
court:.....
.....

Having considered the application, (tick one):

I am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice. ☐

I refuse to approve the grant or renewal of the authorisation/notice. ☐

I refuse to approve the grant or renewal and quash the authorisation/notice. ☐

Notes

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Reasons

.....
.....
.....
.....
.....

.....

.....
.....

.....
.....

.....
.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Appendix G

Contact details for Her Majesty's Courts and Tribunal Service (HMCTS) Gloucestershire

During normal office hours, the court support section should be contacted either by phone or email. There number is 01452 420174 and email is gs-glosmcadmin@hmcts.gsi.gov.uk.

The police have lists of those legal advisers that are contactable out of hours and in the unlikely situation when an application needs to be made urgently details can be obtained from the custody suites at Cheltenham and Gloucester and also the control room at Waterwells.

Appendix H

Non RIPA Surveillance Application Form

Public Authority *(including full address)*		**Unique NO.**	

Name of Applicant		**Department**	

Contact Details	
Investigation/Operation Name (if applicable)	
Investigating Officer (if a person other than the applicant)	

1. DETAILS OF APPLICATION
Describe the purpose of the specific operation or investigation e.g. Internal Disciplinary Investigation. Provide details of the investigation and intelligence case to date to include enquiries already undertaken and their result.
2. DETAILS OF SURVEILLANCE
Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, video recording equipment) that may be used. **Explain the information that it is desired to obtain as a result of the directed surveillance.**
3. SUBJECT OF SURVEILLANCE
The identities, where known, of those to be subject of the directed surveillance. **Should include where known name, address, D.O.B. or approximate age.** **If persons unknown please provide any description's or other information that may be known.**
4. MISDEMEANOR UNDER INVESTIGATION
Provide details of what offences or malpractice is under investigation, e.g.. Gross Misconduct against. Disciplinary Regulations.

5. INTRUSION AND PRIVACY ISSUES
Detail whether <u>Confidential Information</u> such as information relating to legal privilege, health, spiritual counselling or other sensitive information is likely to be obtained against any personas a result of the surveillance activity. **Supply details of any <u>Collateral Intrusion</u>.** **Why the intrusion is unavoidable.** **Describe precautions you will take to minimise and manage the collateral intrusion.**
6. NECESSITY AND PROPORTIONALITY
Explain why it is necessary to use the covert methods applied for, can the evidence be obtained by less intrusive methods and explain why this surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?
7. APPLICANTS DETAILS

Name (print)		**Tel No:**	
Grade/Position		**Date Submitted**	
Signature			

<u>AUTHORISATION SECTION</u>
8. AUTHORISED YES OR NO? (see below)
If rejected detail the reason why. **If authorised state exactly what activity is being authorised by whom and if necessary what equipment they are authorised to use and in what circumstances. This should include any specific instructions such as the management of any images which may be obtained. Cover who, what, where, when and how.**
9. NECESSITY AND PROPORTIONALITY
Explain why you believe the surveillance is necessary and proportionate to what is sought to be achieved by carrying out the covert activity.
10. CONFIDENTIAL INFORMATION

If confidential information is likely to be obtained (see box 5) state how the information will be managed and disposed of. (Seek advice from legal section and data controller if required). May require a higher level of authority.
11. DATE OF FIRST REVIEW
Set a review date taking into account all the circumstances. The review date should be no longer than a month to demonstrate that the process is being managed effectively

Date	

12. AUTHORISING OFFICER DETAILS			
Name (Print)		**Grade/Position**	
Signature		**Time and Date**	

April 2016

Policy and Procedures Document for the acquisition of Communications Data using The Regulation of Investigatory Powers Act 2000 (RIPA)

CHELTENHAM
BOROUGH COUNCIL

www.cheltenham.gov.uk

CONTENTS

1. BACKGROUND

1.1. The Council has a procedural guide for the use of RIPA which has been in place for some time and it should be noted that this document does not replace it. Any officer considering the use of RIPA as part of an investigation should follow the original guidance in the first instance.

1.2. Since September 2014, Local Authorities can only access communications data via the National Anti-Fraud Network (NAFN):

'NAFN is a not-for-profit, non-incorporated body formed by its members to provide services which support their work in the protection of the public purse. Established in 1997, NAFN was created as a centre of excellence to provide data and intelligence to its members. This includes assisting members in the provision of effective corporate and financial governance.

NAFN works with its members and other stakeholders to enhance and expand its range of services. It maintains all data in a secure and confidential environment conforming to Government legislation and national best practice'
NAFN constitution

1.3. Whilst it is not compulsory to join NAFN per se, a Local Authority must be a paid up member in order to make use of its single point of contact (SPoC) service in relation to communications data. The Council is a member, primarily to make use of other services provided by NAFN (credit referencing, DVLA checks, debtor tracing etc.) but given that Officers could now utilise the RIPA SPoC service and obtain communications data, guidance needs to be in place to govern the process.

1.4. This procedural guide is based on the requirements of The Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office Code of Practice on the Acquisition and Disclosure of Communication Data. The Council takes responsibility for ensuring its RIPA procedures are continuously improved and asks that any Officers with suggestions contact the RIPA Coordinator in the first instance. If any of the Home Office Codes of Practice change, the appropriate guide will be updated, and the amended version placed on the internet / published accordingly. Regular training sessions will also be provided to ensure that staff members are fully conversant with the Act.

1.5. Part 1 Chapter 2 of RIPA controls the obtaining of communications data by Local Authority staff. This data does not include the content of the communications i.e. the actual email message, letter, text or telephone conversation.

1.6. Part 1 also introduces a statutory framework to regulate access to communications data by Public Bodies consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in these processes. In addition it puts safeguards in place to balance the rights of the individual against the needs of society, as a whole, to be protected from crime and other public safety risks. This thus reflects the requirements of Article 8 of the European Convention on Human Rights; the right to privacy.

1.7. Communications data obtained under RIPA will be a justifiable interference with an individual's human rights, as above, provided such conduct is authorised, is both necessary and proportionate, and is in accordance with the law.

1.8. Therefore no Officer of the Council should require or invite a postal or communications operator to disclose data through the use of any other statutory duty or by exercising an exemption to the principle of non-disclosure under the Data Protection Act 1998. Another statutory power may only be used if it explicitly provides for the obtaining of telecommunications data.

1.9. In terms of internal monitoring of communications data, emails, internet usage etc. it is important to recognise the interplay and overlap with the Council's ICT Policies and the Data Protection Act 1998 (to include the Codes of Practice). Under normal circumstances the Council's Policies should be adhered to as any such monitoring is permitted as per Contracts of Employment and Codes of Conduct. All electronic data held internally is deemed to be of a business nature and may therefore be accessed without further notice; RIPA authorisation is not therefore required. However, advice should be obtained if there are any significant implications which could impact a person's private life. In those circumstances it may be prudent to complete a Non-RIPA Authorisation Form to consider any human rights issues which must be retained on the central register.

2. DEFINITION OF COMMUNICATIONS DATA AND CATEGORISATION

2.1. Communication data means any traffic or any information that is or has been sent over a communications system or postal system, together with information about the use of the system made by any person. In effect the term communications data embraces the "who, when and where" of a communication but not the content, not what was said or written. It can include the address on an envelope, the time and duration of a communication, the telephone number or e- mail address of the originator and recipient, unanswered call attempts and the location from which the communication was made. It includes the manner in which and by what method a person (or machine) communicates with another person (or machine), but excludes what they say or data they pass on, including text, audio and video. The content of such communications is covered by Interception of Communications Legislation.

2.2. An operator who provides a postal or telecommunications service is described as a Communications Service Provider (CSP).

2.3. Section 4 of the Data Retention and Investigatory Powers Act 2014 (DRIPA) clarifies that data access powers under RIPA are exercisable in respect of CSPs that are based outside of the United Kingdom, but provide services to the UK. Data retained under a Data Retention Notice under Section 1 of DRIPA can only be acquired in accordance with RIPA (or a Court Order).

2.4. RIPA defines communications data in three broad categories:

- Section 21(4)(c) Information about Communications Service Users:

This category is information held or obtained by a CSP about persons to whom communications services are provided. It mainly includes personal records supplied to the Communication Services Provider (CSP) by the customer/ subscriber. For example, their name and address, payment method, contact number etc.

- Section 21(4)(b) Information about the use of Communications Services:

This category is the data relating to the use made by a person of a communications service. It mainly includes everyday data collected by the CSP related to the customer's use of their communications system and which would be routinely available to the customer. For example, details of the dates and times they have made calls and which telephone numbers they have called.

- Section 21(4)(a) Information about Communications Data (Traffic Data):

This category is data that is or has been comprised in or attached to a communication for the purpose of its transmission. It mainly includes data generated by the Communications Service Provider (network data) relating to a customer's use of their communications system (that the customer may not be aware of), for example, cell site data and routing information.

3. COMMUNICATIONS DATA AVAILABLE TO LOCAL AUTHORITIES

3.1. The types of information that we are allowed to access from a CSP fall into two categories:

- Subscriber Information (RIPA S21(4)(c)) - Information about Communications Services Users:

Name of the customer who is the subscriber for a telephone number, an email account, PO Box number, a Post Paid mailing stamp, or is entitled to post to a web space;

Account information such as address for billing, delivery or installation;

Subscriber account information such as bill paying arrangements, including details of payments and bank or credit/ debit card details;

Information about the provision of forwarding and redirection services;

Information about connection, disconnection and reconnection of services the customer subscribes to, including conference calling, call messaging, call waiting and call barring telecommunications services;

Information provided by the subscriber to the CSP such as demographic information or sign up data (other than passwords) such as contact telephone numbers;

Information about telephones or other devices provided by the CSP to the subscriber and associated codes, including manufacturer and model, Personal Unlocking Keys for mobile phones & serial numbers;

Information that the CSP chooses to collect about the device being used by the customer;

Top-up details for pre-pay mobile phones including credit/ debit card, voucher/ e-top up details.

- Service Use Data (RIPA S 22(4)(b) - Information about the use of Communications Services:

Periods during which the customer used the service;

Activity including itemised records of telephone numbers called, Internet connections, dates and times of calls, duration of calls, text messages sent and quantities of data uploaded or downloaded;

Information about use made of forwarding and redirection services;

Information about the use made of conference calling, call messaging, call waiting and call barring telecommunications services;

Information about the selection of preferential numbers or discount calls;

Records of postal items; such as records of registered, recorded or special delivery postal items and records of parcel consignment, delivery and collection.

3.2. The Council is not allowed to access:

- Traffic Data (RIPA S 22(4}(a) - Information about the communications themselves:

Information identifying the sender and recipient of a communication (from data within the communication);

Information tracing the origin or destination of a communication including incoming call records;

Information identifying any location of any equipment making a communication, such as mobile phone cell site location;

Web browsing information such as the web sites visited (rather than the specific pages within that website) or servers used;

Routing information identifying equipment through which a communication has been transmitted (e.g. dynamic IP addresses, file transfer logs and email headers);

Addresses or markings, including sender or recipient, written on the outside of a postal item in transmission (such as a letter or parcel), that shows the items postal routing;

Online tracking of Communications, such as postal items.

3.3. Local Authority staff are only allowed to acquire and disclose communications data for the purpose of preventing or detecting crime or for preventing disorder. This

purpose should only be used in relation to the specific (and often specialist) offences or conduct that the Council has been given the statutory function to investigate. For communications data, the offence does not have to carry a six month tariff as with directed surveillance.

3.4. Where a joint investigation is being conducted between the Council and another enforcement authority, such as the police, either authority may, where necessary and proportionate, acquire any communications data under RIPA to further the joint investigation.

3.5. The purpose of this policy is to provide guidance for obtaining communications data now that the Council is a member of NAFN. The knowledge and experience of the NAFN Single Points of Contact (SPoC's) is essential and these SPoC's should be used to obtain advice and assistance as and when required. Such a discussion is particularly helpful when the Applicant is unsure of the category of data that they are seeking or the Applicant wants to find out more about what additional information may be retained by the CSP. However, final approval of the request is made by an authorising member of staff; the Designated Person(s) within the Local Authority.

4. POWER TO OBTAIN COMMUNICATIONS DATA

4.1. There are two powers granted by S22 RIPA in respect of the acquisition of communications data from telecommunications and postal companies or 'Communications Service Providers' (CSP's).

4.2. A notice under S22(4). In order to compel a CSP to obtain and disclose, or just disclose, communications data in their possession, a notice under S22(4) RIPA must be issued. The sole grounds to permit the issuing of a S22 notice by a Local Authority is for the purposes of 'preventing or detecting crime or of preventing disorder'. The issuing of such a notice is likely to be the main power utilised by a Local Authority, in those circumstances where the Council SPoC, being NAFN, liaises directly with the CSP.

4.3. An authorisation under S22(3). This power is to be used when a CSP cannot provide the information; there may be several reasons for this. An authorisation provides for persons within a public authority to engage in specific conduct, relating to a postal service or telecommunications system, to obtain communications data. Any designated person in a public authority may only authorise persons working in the same public authority to engage in specific conduct, such as requesting the data via secure auditable communications data acquisition systems. This will normally be the public authority's SPoC, though Local Authorities must now use NAFN.

4.4. Under S23A and S23B RIPA, judicial approval must also be granted for all Local Authority requests for communications data. This is outlined in more detail within this policy.

5. PROCEDURE FOR OBTAINING COMMUNICATIONS DATA

5.1. There is now only one method that officers can use to obtain communications data; by way of the NAFN secure website. To use this system Applicants have to

individually register on the NAFN website - www.nafn.gov.uk. A Designated Person will also need to be registered to authorise the Applicants requests. A number of departments within the Council have contributed towards the NAFN annual membership fee, any Applicant therefore needs to confirm with their Line Manager that they are allowed to register. Should you have any queries, please contact the Internal Audit Department.

5.2. Please note, if your department is part of a shared service, the Local Authority on whose behalf the request is being made must be a member of NAFN and the request made via login details for that Council. Applicants and Designated Persons cannot make use of one Local Authority's membership to obtain any information on behalf of another. Login details will be necessary for each Local Authority that an individual is employed by or works on behalf of.

5.3. Once an Applicant is registered with NAFN, as with other RIPA requests, the Applicant must complete an application for the communications data. This request is completed online and is submitted electronically to the SPoC's at NAFN. On this form the Applicant must provide the following information:

- Name and designation of Applicant;
- Include a unique reference number and, where applicable, the operation name;
- The purpose for which the data is required, which can only be for the prevention and detection of crime or preventing disorder;
- Details of the communications data required;
- Describe whether the communications data relates to a victim, a witness, a complainant, a suspect, a vulnerable person or other person relevant to the investigation;
- Time period for which the data is required, including historic or future data;
- Why it is necessary to obtain the data, including the source of the communications data address and what is expected to be achieved from obtaining the data;
- Why it is proportionate for the data to be obtained, including why the intrusion benefits the investigation and whether the level of intrusion can be justified against the individual's right to privacy;
- Details of whether there is any meaningful collateral intrusion and why that intrusion is justified;
- Consider and describe any possible unintended consequences of the application;
- Time scale within which the data is required (this can only be the routine non-urgent timescale i.e. Grade 3, unless there is a high level of urgency for obtaining the data, such as when life is in danger);
- The Applicant also confirms that they undertake to inform the SPoC of any changes in circumstances that no longer justify the acquisition of the data.

5.4. As with all RIPA applications, a request for communications data should only be made after all other avenues have been considered. It is therefore appropriate that the Applicant should indicate any open source checks that they have made on the

telephone numbers/ communications addresses already made to justify the principle of proportionality.

5.5. The Applicant is entitled to ask for historical data or may request future data, by which the CSP must provide details of, for example, all outgoing telephones or internet connections over a set future period of up to a month. Requests for such future data are considered to be more intrusive than requests for historical data.

5.6. It can be appropriate to obtain service use data at the same time as obtaining subscriber information, for example when the person who is the subject of the investigation is identified from high-grade intelligence to be using a specific number or service or when a mobile phone is lawfully seized. An application for subscriber information can be included in an application for service use data.

5.7. Once fully complete, the form can then passed electronically to the appropriate NAFN accredited Single Point of Contact for Accessing Communications Data (SPoC). The accredited SPoC's at NAFN provide independent scrutiny of the applications so it is important that the Applicant consults with a NAFN SPoC throughout the authorisation process. The NAFN SPoC will advise the Applicant of any amendments necessary.

5.8. After the NAFN SPoC considers the application to be satisfactory, the appropriate Designated Person will then receive an email to say that there is an application form on the website for him or her to consider. The Designated Person completes the relevant part of the form to provide approval.

5.9. At this time, the RIPA Coordinator / Senior Responsible Officer should be made aware that a request has been made so that the central register can be updated.

5.10. The NAFN SPoC then uses the authorisation process to obtain the required communications data from the CSP database. The data is posted on the NAFN website and can only be accessed by the Applicant. If NAFN do not have direct access to the database of the relevant CSP, the NAFN SPoC will send a notice to the CSP in the usual way.

5.11. The majority of information related to public sector business, operations and services can be managed as OFFICIAL; in the case of communications data this should be managed as OFFICIAL – SENSITIVE which identifies it as being subject to a 'need to know' basis thus limiting access to it. This does not preclude the lawful disclosure of material when required but does make clear that the information obtained must be treated with care, and also stored and handled in accordance with the Council's duties under the Data Protection Act.

5.12. Using NAFN to obtain communications data has significant advantages in comparison to the previous method in that the time in which the data can be obtained is significantly reduced, costs are kept to a minimum because the charges made by the CSP's for providing the data are considerably less when using NAFN and it ensures consistency across Local Authorities.

6. COMMUNICATIONS DATA RELATING TO CERTAIN PROFESSIONALS

6.1. Communications data is not subject to any form of professional privilege, since the fact that a communication has taken place does not disclose its contents. Clearly though the degree of interference with privacy may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (for example a medical doctor or lawyer). It may also be possible to infer an issue of sensitivity from the fact that someone has regular contact with someone like a lawyer or journalist.

6.2. Such situations do not preclude an application being made. Special consideration should be given to the issues of necessity and proportionality, drawing attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly privacy, and where it might be engaged, freedom of expression.

6.3. Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That such an application has been made must be recorded, to include the profession, and, at the next inspection, such applications should be flagged to the Interception of Communications Commissioner's Office (IOCCO).

6.4. Issues surrounding the infringement of the right to freedom of expression may arise when a request is made for the communications data of a journalist. There is a strong public interest in the willingness of sources to provide information to journalists anonymously. If an application is intended to determine the source of journalistic information, there must be an overriding requirement for it to be in the public interest. Even if it is not intended to determine the source of journalistic information there is still a risk of collateral intrusion into legitimate journalistic sources, so particular care should be taken to properly consider the public interest in whether the intrusion is justified. This should include drawing attention to whether alternative evidence exists or whether there are alternative means to obtain the information. Identification of journalist sources can only be sought by using production orders under the Police and Criminal Evidence Act 1984 (PACE), which are not available to the Council. Judicial oversight does not apply where applications are made for the communications data of those known to be journalists, but where the application is not to determine the source of journalistic information, for example where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation.

6.5. Communications data that may be considered to determine journalistic sources includes data relating to:

- Journalists' communications addresses;
- Communications addresses of those persons suspected to be a source;
- Communications addresses of persons suspected to be acting as intermediaries between the journalist and the suspected source.

7. PREPAID MOBILE PHONES

7.1. Unregistered prepaid mobile phones are common amongst criminals as it allows them to avoid detection more easily and it is thus possible that a subscriber check will identify a number as belonging to one of these devices. This does not necessarily prevent an investigating officer obtaining useful information.

7.2. The Applicant can ask for further information about the subscriber under section 21(4)(c) including top-up details, method of payment, bank account used or customer notes.

7.3. The Applicant should outline in their original application the further information that will be required if the phone turns out to be prepaid, so as to allow the widening of the data capture. This information could be requested in two stages: firstly asking for the subscriber details and then, if this turns out to be an unregistered prepaid phone, asking for the further information.

7.4. If the Designated Person approves the application it is recommended by IOCCO that he or she should approve the use of authorisations rather than the use of notices, whereby the authorisation should state that the SPoC is authorised to engage in any conduct to acquire information about the user that is covered by Section 21(4)(c). Under the legislation an authorisation does not have to be issued by the Designated Person so it can be issued by the SPoC.

7.5. The SPoC will then serve an appropriate authorisation on the relevant CSP. If further information is required the SPoC will need to serve another authorisation on the CSP requesting the additional information. It should be noted that each authorisation will bear the date that the Designated Person approved the original application. This streamlining process is more efficient than using notices, because otherwise a request for each additional notice would need to be referred to the Designated Person.

7.6. The information that is received can then be developed to try to obtain further information about the user of the phone. Solution Providers such as EasyPay, EPay etc. are the third parties involved in the transaction of credit placed on a mobile phone. If a Solution Provider is provided with the mobile telephone number, the transaction date and the transaction number, they are often able to provide the method of payment and the location of the top-up. Solution Providers are not CSPs and therefore they cannot be issued with a notice under RIPA; instead the data can be applied for under the Data Protection Act.

8. HOME OFFICE GUIDANCE

8.1. The Home Office has provided guidance in relation to the acquisition of communications data namely ‘Guidance for the layout of a Chapter II Application Form and; Guidance for Applicants and Designated Persons considering necessity and proportionality’.

8.2. The guidance was produced jointly by the Home Office and the Data Communications Group (DCG) in conjunction with the IOCCO. The full document is available online should it be required.

8.3. The Home Office also produced a Code of Practice and various revisions have taken place. Relevant extracts are detailed below taking in to account the guidance and Code of Practice. The Council and those persons acting under RIPA must have regard to the Code of Practice on the Acquisition and Disclosure of Communications Data issued by the Home Office under the Act. The full document is available online.

8.4. **COMMUNICATIONS DATA:** An application, comments by the Single Point of Contact (SPoC), considerations of the Designated Person, authorisations and notices may be made in writing ('paper') or electronically ('database').

8.5. It may be appropriate for the section 'communications data' within the application form to include 'text boxes' to enable the applicant to set out the:

- Telephone number, email address, etc;
- Where appropriate the 'between times/ dates' of the data set required;
- Type of data required, for example subscription details, outgoing calls, incoming calls.

8.6. An application may contain several requests for various 'data sets' relating to a specific investigation or operation. However, consideration should be given as to how this may affect the efficiency of the public authority's processes and the impact of managing disclosure issues before, during and after a criminal trial.

8.7. **NECESSITY:** In order to justify the application is necessary the applicant needs as a minimum to consider three main points:

- The *event* under investigation, such as a crime or vulnerable missing person;
- The p*erson*, such as a suspect, witness or missing person and how they are linked to the event;
- The *communication data*, such as a telephone number or IP address, and how this data is related to the person and the event.

8.8. In essence, necessity should be a short explanation of a) the event, b) the person and c) the communications data and how these three link together. The application must establish a link between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

8.9. Necessity does not entail explaining 'what will be achieved by acquiring the data' or 'why specific time periods have been requested' - these points are relevant to proportionality and should be covered in the relevant section to stop repetition.

8.10. **PROPORTIONALITY:** Applicants should include an outline of how obtaining the data will benefit the investigation or operation. If more than one item of data is being sought, the relevance of the additional data should be explained.

8.11. This outline should include explaining how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example the subscriber details of

a phone number may be obtained from a phone book or other publically available source.

8.12. The relevance of any time periods requested must be explained, outlining how these periods are proportionate to the event under investigation. The two basic questions are:

- What are you looking for in the data to be acquired and;
- If the data contains what you are looking for, what will be your next course of action.

8.13. An explanation as to how communications data will be used, once acquired, and how it will benefit the investigation or operation, will enable the Applicant to set out the basis of proportionality.

8.14. An explanation of the proportionality of the application should include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

8.15. An examination of the proportionality of the application should also involve consideration of possible unintended consequences and, when relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application. Unintended consequences are more likely in applications for the data of those professions with duties of confidentiality. For example, if a journalist is a victim of crime, applications for service use data related to that journalist's phone number as part of the criminal investigation may also return some phone numbers of that journalist's sources, with unintended impact on freedom of expression. Such an application may still be necessary and proportionate but the risk of unintended consequences should be considered.

8.16. **COLLATERAL INTRUSION:** Consideration of collateral intrusion forms part of the proportionality considerations and becomes increasingly relevant when applying for traffic data or service use data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion. When there are no meaningful collateral intrusion risks, such as when applying for subscriber details of the person under investigation, the absence of collateral intrusion should be noted.

8.17. The question to be asked is ‘Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for?’ For example itemised billing on the subject's family home will be likely to contain calls made by the family members.

8.18. Applicants should not write about a potential or hypothetical ‘error’ and if the Applicant cannot identify any meaningful collateral intrusion, that factor should be recorded in the application i.e. ‘none identified’.

8.19. **TIME SCALE:** Completion of this section within the application form assists the SPoC to prioritise the request.

8.20. DCG has an agreed Grading System that indicates to the CSP any urgent timescales, which is synchronised with the Urgent Oral Process (see Home Office Acquisition and Disclosure of Communications Data Code of Practice).

8.21. **ROLE OF THE SPOC:** The Home Office must accredit all SPoCs, and this involves attendance on a recognised training course, the passing of an examination and being issued with a SPoC Personal Identification Number. The SPoC ensures that only practical and lawful requests for communications data are undertaken.

8.22. All notices and authorisations for communications data must be channelled through SPoC at NAFN. This is in order to provide an efficient regime since the SPoC will deal with the CSP's on a regular basis.

8.23. The SPoC (in this case NAFN) will receive the application form and will advise Applicants and Designated Persons on the following:

- Whether the forms have been filled in correctly and are lawful;
- Whether the data requested falls within Section 21(4) (a), (b) or (c) of the act;
- Whether access to the communications data is reasonably practical for the CSP or whether the specific data required is inextricably linked to other data;
- Whether there are likely to be any possible unintended consequences of the application;
- The practicalities of accessing different types of communications data from different telecommunications or postal operators;
- Whether data disclosed by a CSP fulfils the requirements of the notice;

8.24. The SPoC will assess the Application for Communications Data form and on it record the following:

- If the request is not reasonably practical for the SPoC the reason why this is so;
- Whether the data falls into Section 21(4) (a), (b) or (c) of the act;
- Whether a notice or authorisation is appropriate;
- Any adverse cost implications to the CSP or the Local Authority;
- Details of any data that is likely to be obtained in excess of the data requested;
- Any other factors that the Designated Person should be aware of;
- Description of the data to be acquired and, where relevant, specifying whether any historic or future data is required and the time periods sought;
- Identifying the relevant CSP.

8.25. The SPoC will issue a Unique Reference Number for the form. The SPoC will draft the relevant notice or authorisation to be submitted for approval to the Designated Person. The SPOC will keep a chronological record of the processing of the application including any contacts made by him or her with the CSP's. He or she may also give a priority grading to the CSP depending on the urgency of the application.

8.26. NAFN employ a number of officers as SPoCs and they can be contacted directly at the NAFN Offices to discuss any issues.

8.27. If the Council needs to request information from a CSP that does not consist of communications data, it is good practice to use the NAFN SPoC to liaise with the CSP on such requests.

8.28. **CONSIDERATIONS OF THE SPOC:** If the application is being recorded within a database (or other electronic format), and is attributable to the applicant, a signature is not required.

8.29. An application, comments by the single point of contact (SPOC), considerations of the Designated Person, authorisations and notices may be made in writing ('paper') or electronically ('database').

8.30. The question 'Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought', is appropriate where the communications data sought by the Applicant may need refinement by the SPOC. For example incoming calls to a telephone number held by a CSP that does not keep a data set that can reveal such calls. The SPOC would state that several authorisations and notices will need to be undertaken with CSPs that can reveal calls instigating from the networks to the telephone number in question.

8.31. The Designated Person, having considered the comments of the SPoC, may decide the acquisition is not justified because of the significant resources required by the CSP to retrieve and disclose the data or it will be impractical for the public authority to undertake an analysis of the data.

8.32. It will also be appropriate for the SPoC to comment where the data sought by the Applicant will require the acquisition of excess data, specifically where it is not practicable for the CSP to edit or filter the data, for example a specific incoming call in a data set with outgoing calls and cell site contained in it. If the Designated Person considers this to be necessary and proportionate for the acquisition of the specific incoming call then the authorisation or notice must specifically include the acquisition of the outgoing call, incoming calls and cell site.

8.33. **APPROVAL BY THE DESIGNATED PERSON:** The SPoC will submit the Application for Communications Data Form, along with the relevant draft notice(s) or authorisation(s), to a Designated Person, who will make the decision about whether or not the application will be approved.

8.34. The Designated Person must be one of those officers, of a suitable rank, who are currently Authorised Officers under RIPA, so they are already able to approve surveillance or CHIS applications. In no cases may someone be both the Designated Person and the Applicant.

8.35. Designated Persons must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data.

8.36. Designated Persons must be independent from the operation or investigation when granting authorisations or giving notices relating to those operations. The Designated

Person must not be directly responsible for the operation or investigation i.e. they should not have a strategic or tactical influence on the investigation. In effect the Designated Person should be far enough removed from the Applicant's line management chain, which will normally mean they are not within the same department or unit. The name of the Designated Person will be given to NAFN and any application requiring approval will be sent direct.

8.37. In circumstances where the Council is not able to call on the services of an independent Designated Person, the Senior Responsible Officer must inform IOCCO of the circumstances and reasons. This could include a small specialist investigation service within the Council, for example applications which relate to corporate fraud and/or internal investigations. The justification for using a non-independent Designated Person and their involvement in the investigation must be explicit in their recorded considerations. Any use of non-independent Designated Persons must be notified to IOCCO during any inspections. The submission to IOCCO of the notification of exemption form is considered to be sufficient for these purposes.

8.38. The Designated Person will consider the form and then complete the Designated Person's part of the Application Form to state whether they grant or refuse the application. On the form the Designated Person must record the following:

- Why he/she believes acquiring the communications data is necessary;
- Why he/she believes the conduct involved in acquiring the communications data is proportionate;
- If accessing the communications data involves a meaningful degree of collateral intrusion, why he/she believes that the request is still proportionate.

8.39. When considering proportionality the Designated Person should apply particular consideration to unintended consequences.

8.40. The decision of the Designated Person must be based on the information presented to them in the application. If the application is approved, the Designated Person can authorise the accessing of communications data by one of two methods as follows:

- By a notice under RIPA S 22(4), which is a notice given to the postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the Authority that served the notice.
- By an authorisation under RIPA S 22(3), which allows the Authority to collect and retrieve the data itself. It is extremely unlikely that we will make use of this, as this is only intended to be used if the operator is incapable of complying with a notice, or if the Authority will retrieve the data using an on-line system.

8.41. The Designated Person should specify the shortest time period for the data that is necessary in order to achieve the objective for which the data is sought.

8.42. The Designated Person shall endorse the draft notice or authorisation with the date, and if appropriate the time, at which he or she gives the notice or authorisation. This is the point at which the Designated Person approves the application.

8.43. If the Designated Person wishes for any advice they are able to obtain it from the NAFN SPoC.

8.44. At the time of giving a notice or granting an authorisation to obtain specific service use information, the Designated Person may also authorise the consequential acquisition of specific subscriber information relating to the service use data that is to be obtained. This must only be to the extent that is necessary and proportionate at that time, such as to identify with who a person has been in communication.

8.45. If the application is rejected either by the SPoC or the Designated Person, the SPoC will retain the form and inform the Applicant in writing and include the reasons for its rejection. The RIPA coordinator will also need to be informed of any rejected applications so that the central register can be updated.

8.46. Once the application has been authorised by the Designated Person the authorisation then needs to receive judicial approval from a magistrate. Further information is set out at within the section detailed 'Judicial Approval'.

8.47. **CONSIDERATIONS OF THE DESIGNATED PERSON:** The Designated Person must be able to show he or she has understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny.

8.48. The Designated Person should tailor their comments to a specific application as this best demonstrates the application has been properly considered.

8.49. If the Designated Person having read the application considers the Applicant has met all requirements, then he or she should simply record that fact. In such cases a simple note by the Designated Person should be recorded.

8.50. There may be circumstances where the Designated Person having read the case set out by the Applicant and the considerations of the SPoC will want to comment why it is still necessary and proportionate to obtain the data despite excessive data being acquired.

8.51. If the Designated Person does not consider the case for obtaining the data has been met the application should be rejected and referred back to the SPoC and the Applicant.

8.52. A notice must include a unique reference number that also identifies the public authority. This can be a code or abbreviation.

8.53. If the Designated Person is recording their considerations within a database (or other electronic format) and is attributable to the Designated Person, a signature is not required.

8.54. **NOTICES AND AUTHORISATIONS:** The NAFN SPoC will supply the Designated Person with a draft notice or authorisation. Where a notice needs to be issued, the NAFN SPoC will produce the notice on behalf of the Designated Person. All notices and authorisations should refer to data relating to a specific date or period of time. If the date is specified as 'current', the data should be provided by the CSP as at the

date of the notice. The notice should give enough information to the CSP to allow them to comply. There is no need to produce a separate notice for each communications address, when these addresses all relate to the same CSP.

8.55. The notice is then served on the CSP by the relevant SPoC. The SPoC will give the notice a Unique Reference Number that cross-references it to the application that was granted.

8.56. The SPoC is responsible for all contacts between the Authority and the CSP.

8.57. Authorisations will mainly be utilised when carrying out the streamlining process for prepaid phones. The SPoC will generate the authorisation on behalf of the Designated Person. The NAFN SPoC will be able to obtain the communications data from the CSP database. Legally the authorisation does not need to be served on the CSP. However the CSP may require or be given an assurance that the conduct undertaken is lawful. That assurance may be given by disclosing details of the authorisation or by providing the actual authorisation.

8.58. Once the data is obtained, the SPoC will provide the data to the Applicant, but the SPoC can filter out any unnecessary information provided by the CSP. The SPoC will retain the original data obtained from the CSP (known as the 'golden copy') and provide a copy of it to the Applicant. This golden copy is capable of being provided to the CSP in the future, in order to enable a witness statement to be obtained in circumstances where the CSP no longer retains their original data. The Applicant should keep the data that they receive in a secure manner, in order to comply with Data Protection requirements.

8.59. The CSP must comply with the requirements of a notice, as long as it is reasonably practical for them to do so. Under S24 of RIPA, the CSP is entitled to recover the reasonable costs of making 'timely disclosure' of such data. Ordinarily the CSP should disclose the required communications data within ten working days of the notice being served on them, but if in specific circumstances where this would not be possible the Designated Person may specify a longer period of up to a month.

8.60. All notices and authorisations will only be valid for a month, but they may be renewed by the Designated Person for further periods of a month, at any time within the current life of the notice or authorisation. This should be set out by the Applicant in an addendum to the original application.

8.61. If the need for the communications data ends, or obtaining the data is no longer proportionate, the Designated Person must cancel the notice using a cancellation form, before data is provided by the CSP. This cancellation notice is sent to the CSP.

8.62. In a similar manner an authorisation must be withdrawn and, if appropriate, the CSP should be advised of this withdrawal. In the NAFN system this is done via the website. However the notices (and authorisations) terminate when the CSP provides the requested data, so there is usually no need for a cancellation form to be completed.

8.63. All original documents will be retained as required by the business need and in accordance with the Council's data retention policies.

8.64. **JUDICIAL APPROVAL:** Once an application for the acquisition and use of communications data has been authorised by the Designated Person, the authorisation or notice then needs to receive judicial approval from a Magistrate. The Applicant will need to download the authorised version of the application form from the NAFN website along with the judicial approval forms and take these forms to the Magistrates' Court.

8.65. The Applicant will need to contact the Magistrates' Court to arrange an appointment for the application to be made. The Applicant will complete the judicial approval application form (Form JA1) and prepare a judicial approval order form (Form JA2) for signature by the Justice of the Peace (JP). The application form will contain a brief summary of the circumstances of the case.

8.66. The officer will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon. The original RIPA authorisation should be shown to the JP but it will be retained by the Local Authority. The Court may wish to take a copy. The partially completed judicial application and order forms will be provided to the JP.

8.67. The hearing will be in private and will be heard by a single JP. The JP will read and consider the RIPA authorisation or notice and the judicial application and order forms. He or she may ask questions to clarify points or to require additional reassurance on particular matters.

8.68. The JP will consider whether he or she is satisfied that at the time the authorisation or notice was granted or renewed there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds.

8.69. The forms and supporting papers must by themselves make the case. It is not sufficient for the officer to provide oral evidence where this is not reflected or supported in the papers provided. The JP may note on the form any additional information he or she has received during the hearing but the request should not be submitted in this manner.

8.70. If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation or notice. If an application is refused the Local Authority should consider whether they can reapply using additional information available that had not initially been included within the papers provided at the hearing.

8.71. The JP will record his or her decision on the judicial order form. This will be the official record of the JP's decision. Court staff will securely retain a copy of the RIPA authorisation and the judicial application and order forms.

8.72. The decisions that the JP can make are as follows:

- Approve the grant or renewal of the authorisation or notice;
- Refuse to approve the grant or renewal of an authorisation or notice;
- Refuse to approve the grant or renewal and quash the authorisation or notice.

8.73. If the JP refuses to grant or renew the authorisation or notice it will not take effect and the Local Authority may not use the technique in that case.

8.74. Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the Council going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken. If the JP decides to quash the original authorisation or notice, the court must not exercise its power to quash that authorisation or notice unless the Applicant has had at least two business days from the date of the refusal in which to make representations.

8.75. The Council will need to obtain judicial approval for all initial RIPA authorisations or notices. In addition to the application form etc. officers will need to retain a copy of the judicial application and order forms after they have been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

8.76. On rare occasions officers might have the need for out of hour's access to a JP so the officer will need to make the necessary arrangements with the Court staff. The officer will need to provide two partially completed judicial application and order forms so that one can be retained by the JP. The officer should provide the Court with a copy of the signed judicial application and order forms the next working day.

8.77. Where renewals are timetabled to fall outside of Court hours, for example during a holiday period, it is the investigating officer's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

8.78. Should judicial approval be granted, the officer will need to provide the judicial approval form to the NAFN SPoC.

8.79. **ERRORS:** Where any error occurs, in the giving of a notice or authorisation or as a consequence of any authorised conduct or any conduct undertaken to comply with a notice, a record should be kept. An error can only occur after the notice has been served on the CSP, so if it is discovered before this point it does not officially count as an error. There are two types of errors namely reportable errors and recordable errors:

- Reportable errors are ones where communications data is acquired wrongly and in this case a report must be made to the IOCCO, as this type of occurrence could have significant consequences for the individual whose details were wrongly disclosed. Reportable errors could include:

A notice being made for a purpose, or for a type of data, which the public authority cannot seek;

Human error, such as incorrect transposition of information where communications data is acquired;

Disclosure of the wrong information by a CSP when complying with a notice;

Disclosure or acquisition of data in excess of that required.

- Recordable errors are ones where an error has occurred but has been identified before the communications data has been acquired. The Local Authority must keep a record of these occurrences, but a report does not have to be made to the IOCCO. Recordable errors could include:

A notice which is impossible for a CSP to comply with;

Failure to review information already held, e.g. seeking data already acquired or obtained for the same investigation, or data for which the requirement to obtain it is known to be no longer valid;

Notices being sent out to the wrong CSP;

Human error, such as incorrect transposition of information where communications data is not acquired;

Notices being sent out to CSP's that were not produced by the Designated Person who authorised the application.

8.80. Where a telephone number has been ported to another CSP then this does not constitute an error. Where excess data is disclosed, if the material is not relevant to the investigation it should be destroyed once the report has been made to the IOCCO. This should include destroying copies contained as attachments in emails. If having reviewed the excess material it is intended to make use of it, the Applicant must make an addendum to the original application to set out the reasons for needing to use this excess data. The Designated Person will then decide whether it is necessary and proportionate for the excess data to be used in the investigation. The requirements of DPA and its data protection principles must be adhered to in relation to an excess data.

8.81. Any reportable error must be reported to the Senior Responsible Officer and then to the IOCCO within five working days. The report must contain the unique reference number of the notice and details of the error, plus an explanation how the error occurred, indicating whether any unintended collateral intrusion has taken place and providing an indication of the steps that will take place to prevent a reoccurrence. The 'reporting an error by accredited SPoC form' (CD5) should be used for this purpose.

8.82. If the report relates to an error made by a CSP the Authority must still report it, but should also inform the CSP to enable them to investigate the cause.

8.83. The records kept for recordable errors must include details of the error, explain how the error occurred and provide an indication of the steps that will take place to prevent a reoccurrence. These records must be available for inspection by IOCCO inspectors and must be regularly reviewed by the Senior Responsible Officer.

8.84. The most common cause of errors is the incorrect transposition of telephone numbers, email addresses and IP addresses. In the vast majority of cases these addresses are derived from addresses available to the Applicant in electronic form. Therefore all Applicants are required to electronically copy communications addresses into applications when the source is in electronic form (for example forensic reports relating to mobile phones or call data records etc.) Communications addresses acquired from other sources must be properly checked to reduce the scope for error.

8.85. In circumstances where a reportable error is deemed to be of a serious nature, IOCCO may investigate the circumstances that led to the error and assess the impact of the interference on the rights of the affected person. IOCCO may inform the affected individual, who may make a complaint to the Investigatory Powers Tribunal. The Tribunal has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data.

8.86. **SENIOR RESPONSIBLE OFFICER:** The Senior Responsible Officer is responsible for the following:

- The integrity of the processes of acquiring communications data;
- Compliance with the act and code of practice;
- Oversight of the reporting of errors to IOCCO;
- Engaging with IOCCO inspectors when they conduct inspections;
- Overseeing the implementation of any post-inspection action plans.

8.87. The Head of Paid Service is the Senior Responsible Officer with regard to the acquiring of communications data.

8.88. **CENTRAL RECORDS:** The Council must retain copies of all applications, authorisations, copies of notices and withdrawals of authorisations and cancellation of notices, cross-referenced against each associated document. This will be coordinated by the RIPA Coordination Officer who also holds copies of application for actual surveillance as per the Council's overarching RIPA policy. With the NAFN system, copies of the notices and authorisations are not routinely provided to the Designated Person, but print-offs of the completed online application forms will need to be provided to the RIPA Coordination Officer (consideration must be given to data sharing when dealing with internal investigations). Inspectors from the IOCCO will be able to obtain copies of all of these documents from NAFN.

8.89. The Senior Responsible Officer will have access to all of these forms as and when required.

8.90. The Local Authority must also keep a record of the following:

- Number of applications submitted to the NAFN SPOC;
- Number of applications submitted to the NAFN SPOC which were referred back to the applicant for amendment or declined by the SPOC;
- The reason for any amendments being required or application being declined by the SPOC;

- Number of applications that were approved by the Designated Person;
- Number of applications that were referred back to the applicant or rejected by the Designated Person;
- The reason for any referrals back or rejections;
- Number of notices requiring disclosure of communications data;
- Number of authorisations for conduct to acquire communications data;
- The priority grading of the application for communications data. The Council will only use Grade 3; matters that are routine but where appropriate will include specific or time-critical issues such as bail, Court dates etc;
- Whether any part of the application relates to a person who is member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, MP or minister of religion (and if so, which profession);
- Number of items of communications data sought for each notice or authorisation that was granted;

8.91. For each item of communications data included within a notice or authorisation the Local Authority must keep records of the following additional information:

- The Unique Reference Number of the application, notice and /or authorisation;
- The statutory purpose for which each item of communications data is being requested. The Council is only able to use the purpose of 'preventing or detecting crime or of preventing disorder';
- The type of crime being investigated;
- Whether the communications data is service use information (S21(4)(b) information) or subscriber information (S21(4)(c) information);
- The type of each item of communications data included in the notice or authorisation (such as fixed line telephone data, mobile telephone data or internet data);
- Whether each item of communications data relates to a victim, a witness, a complainant, a suspect, a next of kin, a vulnerable person or other person relevant to the investigation;
- The age of each item of communications data. (If the data includes more than one day, the age will be the oldest date of the data that is sought);
- Where the data sought is service use information on the total number of days of data being sought;
- The CSP from who the data is being acquired. All these records will need to be sent to IOCCO as requested.

8.92. The Lead Officer will keep a database of all applications, plus details of any notices and authorisations whether they are issued by the Local Authority or issued by NAFN on our behalf. This database will include records of any errors that have occurred. NAFN are able to provide on request statistical information about the numbers of notices or authorisations that they have issued.

9. INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

9.1. The exercise of the powers and duties relating to communications data is kept under review by inspectors who work for the Interception of Communications

Commissioner's Office (IOCCO) under the control of the Interception of Communications Commissioner.

9.2. IOCCO state that if we receive a Freedom of Information request for a copy of our inspection report we should notify IOCCO, who will provide us with a suitably redacted version of the report to submit to the requester. No disclosure must take place until IOCCO has been consulted.

10. STRATEGY AND POLICY REVIEW

10.1. The Internal Audit Department will review and amend this policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the vision of the Council.

10.2. Responsible Officer: Head of Internal Audit.
Date: February 2016.

Review frequency as required by legislative changes / every three years.

Information/Discussion Paper

Audit Committee – 23 March 2016

2020 Vision – Residual Corporate Services Matters

Internal Audit Implications

This note contains the information to keep Members informed of matters relating to the work of the Committee, but where no decisions from Members are needed

Why has this briefing come to Audit Committee?

Prior to the Cabinet Meeting on the 9 February the Director of Resources consulted the Audit Committee Chairman on recommendations concerning the delivery of the Internal Audit Service, the Counter fraud Unit and the functions to be delegated to Joint Committee. The Chairman was supportive of the recommendations and agreed that a briefing paper should be brought to this committee in March.

Background

In October 2015 Cabinet and Council approved a number of recommendations to establish the 2020 Vision Joint Committee (hereinafter referred to as the Joint Committee) and for this Council to share more services with the other 2020 partner councils. Cabinet received two reports recommending the delegation of Customer Services, Revenues and Benefits (including Council Tax) functions to the Joint Committee, being new sharing of services arising from the October Cabinet and Council report. During the period since the matter was last considered work has progressed on the creation of the Inter Authority Agreement which will replace the existing legal agreements (s101 agreements) and the GO Shared Services Collaboration Agreement.

Since October, formal consultation has taken place and agreed the Group Manager structure for the 2020 Partnership Venture. These officers have been appointed and will be responsible for the shared services delivered through the Joint Committee and managed by the Partnership Managing Director.

Work on the legal agreements, finalisation of the management structure and work on the performance monitoring framework has therefore led to a number of residual issues being identified which were reported to Cabinet for approval and information as appropriate. Two of these issues related to Internal Audit and the Counter fraud Unit, it was;

RESOLVED THAT

1. Those functions outlined in the Internal Audit Services document attached at Appendix 2 be delegated to the 2020 Vision Joint Committee in accordance with the delegation principles in section 7.

2. Those functions outlined in the Counter Fraud Services document attached at Appendix 3 be delegated to the 2020 Vision Joint Committee in accordance with the delegation principles in section 7.

Audit Committee Members are asked to note the resolutions above, the full cabinet report (Appendix 1) and Appendix 2 that provide detail about the functions to be delegated to the Joint Committee in respect of Internal Audit and the Counter Fraud Unit

Summary of evidence/information

The full cabinet report (Appendix 1) and Appendix 2 which details the functions to be delegated to the Joint Committee in respect of Internal Audit and the Counter Fraud Unit

---

Contact Officer	Bryan Parsons, Corporate Governance, Risk and Compliance officer Tel; 01242 264189 Email bryan.parsons@cheltenham.gov.uk
Accountability	Councillor Jon Walklett, Cabinet Member Corporate Services Mark Sheldon, Director of Resources and Projects

Appendix 1

Cheltenham Borough Council

Cabinet - 9 February 2016

2020 Vision – Residual Corporate Services Matters

Accountable member	**Councillor Jon Walklett, Cabinet Member Corporate Services**
Accountable officer	**Mark Sheldon, Director of Resources and Projects**
Ward(s) affected	**None**
Key Decision	**No**
Executive summary	In October 2015 Cabinet and Council approved a number of recommendations to establish the 2020 Vision Joint Committee (hereinafter referred to as the Joint Committee) and for this Council to share more services with the 2020 partner councils. Cabinet is, at this meeting, receiving two reports recommending the delegation of Customer Services, Revenues and Benefits (including Council Tax) functions to the Joint Committee, being new sharing of services arising from the October Cabinet and Council report. During the period since the matter was last considered work has commenced on the creation of the Inter Authority Agreement which will replace the existing legal agreements (s101 agreements) and the GO Shared Services Collaboration Agreement. Since October formal consultation has now taken place and concluded with regard to the Group Manager structure for the 2020 Partnership Venture. These officers will be responsible for the shared services delivered through the Joint Committee and will be managed by the Partnership Managing Director. Work on the legal agreements, finalisation of the management structure and work on the performance monitoring framework has therefore led to a number of residual issues being identified which are now reported to Cabinet for approval and information as appropriate.
Recommendations	**Cabinet is recommended to** **1. Delegate to the 2020 Vision Joint Committee those functions outlined in the Internal Audit Services document attached at Appendix 2 in accordance with the delegation principles in section 7.** **2. Delegate to the 2020 Vision Joint Committee those functions outlined in the Counter Fraud Services document attached at Appendix 3 in accordance with the delegation principles in section 7.** **3. Agrees the revision to the delegation to the 2020 Vision Joint Committee for ICT services as outlined at paragraph 5.4 and attached at Appendix 4 in accordance with the delegation principles in section 7.** **4. Agrees to appoint West Oxfordshire District Council as the Accountable Body to enter into any contracts required on behalf of the 2020 Vision Joint Committee with regard to the provision of ICT services to Cheltenham Borough Council.** **5. Authorises the Deputy Chief Executive, in consultation with the**

Leader and Cabinet Member Corporate Services, to agree whether and to what extent web and digital services (subject to a business case) should be delegated to the Joint Committee in accordance with the delegation principles in section 7.

6. Authorises the Deputy Chief Executive to undertake all necessary processes and actions and the Borough Solicitor to complete appropriate legal documentation in order to facilitate and implement the matters contained in this report.

Financial implications	There are no immediate direct financial implications arising from this report. However, the delegation of these existing shared services to the Joint committee support the overall programme for which there is a further savings target for support services in phase 3 of the programme i.e. after 2019/20. The programme has a budget of £10m of which £1.5m is set aside for partnership wide investment in business systems to support improvement is services. The proposal to align and deliver a consistent approach to ICT security and data protection across all partner sites will help reduce the net cost of the administrative overhead to the council. **Contact officer: Paul Jones, Section 151 Officer, paul.jones@cheltenham.gov.uk, 01242 775154**
Legal implications	The relationship between the partner councils and the Joint Committee will be set out in the inter-authority agreement which will, inter alia, set out the Joint Committee obligations, the administering authority's obligations, the accountable body's obligations, staffing and exit arrangements. The existing s101s and Collaboration Agreement will be terminated and replaced by the inter authority agreement. Arrangements with Ubico, The Cheltenham Trust and CBH will need to be amended accordingly. The delegation of functions to the Joint Committee will be subject to the overriding principle that the Joint Committee will undertake operational work and that strategic and policy matters (except HR policies) will be retained by the council. **Contact officer: Peter Lewis, Head of Legal, peter.lewis@tewkesbury.gov.uk, 01684 272012**
HR implications (including learning and organisational development)	There are no direct HR implications for Cheltenham Borough Council arising from this report. Secondment agreements are already in place for the two CBC officers who are working as part of Counter Fraud Team. The responsibility for managing HR implications falls to the employing authority for Audit Services (CDC) and for ICT (FoDDC). GOSS HR will provide guidance to those Councils on HR implications as they arise. **Contact officer: Julie McCarthy,** **julie.mccarthy@cheltenham.gov.uk, 01242 264355**

Key risks	The key risks for this Council relates to the need for service standards to be clearly stated in the Joint Committee service plans.
Corporate and community plan Implications	2020 Vision supports the Council's objective of providing value for money services that effectively meet the needs of CBC customers and community.
Environmental and climate change implications	None arising from this report
Property/Asset Implications	None arising from this report **Contact officer: david.roberts 01242 774151, David Roberts@cheltenham.gov.uk**

1. Background

1.1 Since October 2015 when this council considered and approved the recommendations of the 2020 Vision report progress has been made with the necessary arrangements to establish the Joint Committee including

- Detailed scoping of the service functions to be delegated to the Joint Committee
- Finalisation of the Inter Authority Agreement
- Formal consultation on the Partnership Venture Group Management Structure
- Establishing the client and performance management arrangements for monitoring the performance of the services delegated to the Joint Committee.

1.2 The further work undertaken since October has therefore revealed a number of residual issues which now need the approval of Cabinet in order to progress the delegations and finalisation of various legal documentation.

2. Internal Audit

2.1 On 15 November 2011, Cabinet delegated this council's internal audit services to Cotswold District Council, including the transfer of staff under TUPE (Transfer of Undertakings (Protection of Employment).

2.2 Since this council considered the 2020 Vision report and recommendations formal consultation has now taken place and concluded on the Partnership Venture Group Management Structure. The structure includes for a Group Manager responsible for Finance, HR and Audit. Therefore it is proposed that the internal audit functions, as currently carried out under an existing shared service by Audit Cotswolds, be delegated to the Joint Committee.

2.3 The responsibility for the provision of the Audit service will remain with the Section 151 Officer. The scope of internal audit activities proposed to be delegated is shown at **Appendix 2**. Audit Cotswolds do not provide a service to Forest of Dean District Council (FoDDC) who receives their service from SWAP (South West Audit Partnership).

2.4 The council's Audit Committee will be updated on the proposal to delegate the internal audit service at its meeting on 23rd March 2016.

2.5 Under the current s101 agreement the Audit Committee is designated as the Member level group

for monitoring the performance of the current partnership. This is enabled by the fact that the Audit Committee is responsible for ensuring an effective Internal Audit Service as provided under their current Terms of Reference in this council's Constitution.

2.6 The proposal here is therefore that the Audit Committee will remain the designated member level group for the new shared service being delivered by the Joint Committee.

3. Counter Fraud Unit

3.1 On 10 February 2015, Cabinet received a report "Counter Fraud Unit – An Evolutionary Approach, and approved the establishment of a Counter Fraud Unit to be managed by the Council's internal audit provider, Audit Cotswolds.

3.2 The unit is still in embryonic phase with staff seconded to develop work streams which tackle fraud e.g. single person council tax discount using funding provided by DCLG.

3.3 The scope of counter fraud unit activities proposed to be delegated to the Joint Committee is shown at **Appendix 3**.

3.4 A decision to delegate internal audit functions to the Joint Committee would mean that the functions of the Counter Fraud unit would likewise need to be delegated.

3.5 As outlined in the February 2015 Cabinet report the Audit Committee already receives an annual counter fraud report from the Head of Internal Audit and it is proposed that the committee will continue to monitor the work of the unit as delivered by the Joint Committee under the new arrangements. The performance management and governance arrangements have yet to agreed by the partnership.

4. Accountable Body Status for ICT

4.1 The October 2015 report on 2020 Vision stated that Cotswold District Council would be the Accountable Body to enter into any contracts on behalf of the Joint Committee. Operational reasons have resulted in a recommendation that, in the case of ICT contracts only, West Oxfordshire be the contracting authority on behalf of the Joint Committee. All other Joint Committee contracts would be with Cotswold District Council.

5. ICT Service Standards and Performance Indicators

5.1 On 11 December 2012, Cabinet approved the sharing of this council's ICT service with the FoDDC as lead authority from 1 April 2013. In October 2015 it was agreed to delegate to the provision of ICT to the 2020 Vision Joint Committee.

5.2 Whilst ICT is not the subject of a separate cabinet report because it is not a new shared service, since the original business case was written in 2012 there has been considerable change and development within the existing ICT shared service.

5.3 The shared service has focused activity over recent years on implementing the ICT upgrade strategy to address the underinvestment in the council's ICT infrastructure which has resulted in stabilisation of the core ICT infrastructure. This activity has been supported by officers from CDC and WODC which has ensured that the ICT infrastructure across the 4 2020 Vision partner councils is aligned.

5.4 In reviewing the ICT functions to be delegated to the Joint Committee, there is an opportunity to align behind a common approach to ICT security (policies, procedure and advice) which is currently provided by the 2 separate ICTSS for FOD, West Oxford and Cotswold DC but not for Cheltenham where the Corporate Governance Officer provides this role. Similarly, data protection (data handling advice and guidance, policy and management and investigation of security breaches) is currently provided by the 2 separate ICTSS for FOD, West Oxford and Cotswold DC

but not for Cheltenham where the Corporate Governance Officer provides this role. It is proposed that the 4 way ICTSS provides this common service across all partners thereby providing a consistent and cost effective approach for staff working across all sites. This recommendation is reflected in the revised list of ICT functions delegated to the Joint Committee at Appendix 4.

5.5 The service being delegated from day 1 is an 'as is' position i.e. the same level of service currently that is currently being provided. The proposal is for the Group Manager - Customer and Business Support to develop a service plan for the 4 way ICT shared service by June 2016 which will include performance measures to be agreed by the Joint committee for all 4 councils. This will provide an opportunity to revisit the service standards and performance indicators that this council will require to be met by the Joint Committee.

6. Web and digital services

6.1 There is a supporting piece of work being undertaken between Cotswolds, West Oxfordshire and Forest of Dean District Councils to share web and digital services. The project will seek to pool the limited web resource in the three Councils to build a stronger more resilient web-team that is not just concerned with managing day to day activities, but that will also work alongside the Customer Access project and users to develop and improve the digital services to meet customer needs.

6.2 Cheltenham Borough Council has been invited to join the sharing arrangement and officers are currently developing a business case which will consider the merits of remaining in-house alongside the shared option. It is proposed that, subject to the business case, the Deputy Chief Executive, in consultation with the Leader and Cabinet Member Corporate Services, will agree whether and to what extent web and digital services will be delegated to the Joint Committee.

7. Scope of Delegations

7.1 The functions to be delegated to the Joint Committee in respect of Internal Audit and the Counter Fraud Unit are as set out in Appendix 2 and 3. The functions delegated in respect of ICT, including the delegation of data handling and ICT security as per section 5.4) are set out in Appendix 4, with the potential additional delegation of web and digital services (see section 6 above). The Joint Committee will agree its own scheme of officer delegation for delivery of the functions and officers working within the Joint Committee services will operate within that scheme.

7.2 In order to be able to create a functioning service, the Joint Committee and its officers will undertake day-to-day operational decisions regarding the functions that are delegated to it. These include the management of staff and resources (delegated budget) and decisions in respect of the provision of the service e.g. response to emergencies or business interruptions.

7.3 The delegation of the functions to the Joint Committee will be subject to the overriding principle that the Joint Committee will undertake operational work and that strategic and policy matters (except HR policies) will be retained by the council.

8. Reasons for recommendations

8.1 In order to progress the recommendations of the October Cabinet and Council report and to establish the Joint Committee and the shared services.

9. Alternative options considered

9.1 The new shared service business cases have considered alternative delivery options and are subject to separate reports to Cabinet at this meeting.

10. Consultation and feedback

10.1 The Audit Committee will be briefed on 23rd March 2016 with regard to the delegation of internal audit services and the counter fraud unit to the Joint Committee. Overview and Scrutiny have received a discussion paper on the interim client and commissioning arrangements and any feedback will be provided to Cabinet in advance of this meeting.

10.2 Members and staff have taken part in a number of workshops and seminars in the period up to the October Cabinet and Council report and staff workshops are continuing to take place.

10.3 Trade Union and employee representatives are being kept informed of progress through a number of formal and informal meetings. At CBC colleagues have been updated through the Joint Liaison Forum and the Joint Consultative Committee and the GO Shared Services Head of HR and the Partnership Managing Director have meetings with trade union colleagues also.

11. Performance management – monitoring and review

11.1 The Joint Committee Constitution requires the Partnership Managing Director, each year, to submit a 3 year business plan with an annual action plan and the Inter Authority Agreement will also include the relationship between the annual action plan and the service standards and the performance indicators that the Partnership Venture will be monitored against.

11.2 The Inter Authority Agreement will require the Partnership MD to present reports to the partner councils on the effectiveness of the Joint Committee in meeting its performance and efficiency savings targets.

Report author	**Contact officer: Mark Sheldon, Director of Resources and Projects, Mark.sheldon@cheltenham.gov.uk, 01242 264123**
Appendices	1. Risk Assessment 2. Internal Audit Service Scope 3. Counter Fraud Service Scope 4. ICT Service Scope
Background information	1. 2020 Vision Cabinet and Council Report – 13 October 2015 and 19 October 2015 2. Update on sharing services as part of the 2020 Partnership – Overview and Scrutiny Committee 25 January 2016

Risk Assessment

The risk				Original risk score (impact x likelihood)			Managing risk				
Risk ref.	Risk description	Risk Owner	Date raised	Impact 1-5	Likeli-hood 1-6	Score	Control	Action	Deadline	Responsible officer	Transferred to risk register
1	If ICT service standards and performance indicators are not developed the council will be unable to measure the performance of the service.	Pat Pratley	9.2.15	3	3	9	Reduce	The Joint Committee will produce a service plan for ICT / Customer services by June 2016. The IAA contains a requirement for a 3 year service plan.	12.2.15	Pat Pratley	
2	If the process for monitoring the performance of the Joint Committee shared services is not agreed or clear then the performance of the shared services will not be effectively measured.	Pat Pratley	9.2.15	3	3	9	Reduce	The Inter Authority Agreement will include provision for holding the Partnership MD to account for the delivery of the shared services to the required standards and to achieve the agreed performance targets	12.2.15	Pat Pratley	

Explanatory notes

Impact – an assessment of the impact if the risk occurs on a scale of 1-5 (1 being least impact and 5 being major or critical)

Likelihood – how likely is it that the risk will occur on a scale of 1-6

(1 being almost impossible, 2 is very low, 3 is low, 4 significant, 5 high and 6 a very high probability)

Control - Either: Reduce / Accept / Transfer to 3rd party / Close

This page is intentionally left blank

Appendix 2

INTERNAL AUDIT SERVICES

Corporate	
Advice and attendance at meetings in the role as internal auditors to the Council	C / CO / WO
Local Government Law requirements under Accounts and Audit Regulations 2015	C / CO / WO
Regular attendance at Audit Committee or equivalent.	C / CO / WO
Internal Audit advice to Officers and Members in relation to Risk Management, Control and Governance	C / CO / WO
Advice in relation to the governance of the Council.	C/ CO / WO
Dealing with internal Complaints.	C / CO / WO
Investigation of irregularities and impropriety	C / CO / WO
Delivering the CIPFA defined role of the Head of Internal Audit	C / CO / WO
Providing assurance to Audit Committee and Senior Management over all aspects of the Council' governance, Risk Management and Control framework on a risk derived basis	C / CO / WO
Advising on change programmes and projects	C / CO / WO
Advising on corporate initiatives, e.g. shared services/collaborative working	C / CO / WO
Annual Governance Statements – drafting, preparation and testing	C / CO / WO
Audit Team Activity derived from Risk Based Plan and supporting management	
Strategic audits– ensure risk management, governance and controls are in place to help meet organisational objectives	C / CO / WO
Compliance reviews – to ensure stated and approved strategy, policies and procedures are being complied with	C / CO / WO
Operational audits – to ensure systems of internal control are effective, risks are well managed and operations achieve objectives.	C / CO / WO
Regulatory audits – in support of external audit to ensure key financial controls work	C / CO / WO
Investigative work – reactive work in connection with potential fraud, impropriety, breach of policy/procedure etc.	C / CO / WO
Governance audits – ensure an appropriate control framework and governance structure are in place and in line with best practice e.g. Charity Commission, UK Code of Corporate Governance, etc.	C / CO / WO

Financial audits – to ensure appropriate controls are in place and complied with in relation to managing the financial matters of the organisation	C / CO / WO
ICT Audit – to ensure ICT controls are working effectively	C / CO / WO
Contract and Grant Certification audits – to review aspects of the delivery of major contracts or grants – including certification for third parties	C / CO / WO
Value for Money audits – reviewing effectiveness, efficiency, economy and education of any particular activity	C / CO / WO
Environmental audits – assessing the control framework in place to meet environmental objectives	C / CO / WO
Programme and project assurance including gateway reviews	C / CO / WO
Facilitated workshops – governance, control and risk management	C / CO / WO
Productivity reviews – work study / time study based consultancy	C / CO / WO
Risk management advice – including advice on embedding risk management and creating a risk management framework, policy and defining the appetite	C / CO / WO
Counter Fraud Services – access to independent fraud investigators through a dedicated Counter Fraud Unit (See counter fraud services spec)	C / CO / WO
Privacy Impact Assessments – and other Data Protection, information management advice	C / CO / WO
Company governance advice – under the Companies Act 2006 and Financial Reporting Council requirements including Annual Governance Statement framework preparation, review and support	C / CO / WO
Charity governance advice – under the Charities Commission requirements	C / CO / WO
Audit Committee effectiveness reviews – based on CIPFA and IIA principles	C / CO / WO
Due Diligence audits – reviews for investments and service delivery model changes	C / CO / WO
Research – undertake research into related subject areas on behalf of management	C / CO / WO
Shared Services – advice and guidance on shared service governance, control and risk management	C / CO / WO
COUNTER FRAUD UNIT	
Investigate fraudulent CTRS claims and apply appropriate sanction	C / F
Raise debtor accounts for CTRS fraud overpayments/administrative	C / F

penalties if applicable	
Act as SPoC for benefit fraud investigation purposes with DWP	C
Maintain service risk register (Covelent)	CO

This page is intentionally left blank

Audit Committee 2014-2015 work plan

Item	Author	Decision / Discussion
23 March 2016		
Briefing (DSU and Lead officer to agree agenda): 8 February 2016	**Officers and GT liaison:** 7 March 2016	**Reports to DSU by:** 11 March 2016
Audit committee update	Grant Thornton	Discussion
Audit plan (for the current year)	Grant Thornton	Discussion
Annual plan (for the upcoming year)	Lucy Cater	Decision
Internal audit monitoring report (inc. counter fraud update)	Lucy Cater	Decision
Annual review of risk management policy	Bryan Parsons	Decision
Approval of the Code of Corporate Governance	Bryan Parsons	Decision
RIPA guidance review and Acquisition of Communications Data under Regulation of Investigatory powers Act 2000 Policy	Bryan Parsons	Decision
2020 Partnership (residual corporate matters) – this discussion paper will outline the governance arrangements for the 2020 partnership and should include details of the scrutiny arrangements so that any gaps can be identified	Bryan Parsons	Discussion
Annual governance statement (for information only)	Bryan Parsons	Briefing
15 June 2016		
Briefing (to agree agenda): 3 May 2016	**Officers and GT liaison:** 1 June 2016	**Reports to DSU by:** 3 June 2016
Audit committee update	Grant Thornton	Discussion
Internal audit opinion (for the previous year)	Rob Milford	Discussion
Internal audit monitoring report (inc. counter fraud update)	Rob Milford	Discussion
Annual governance statement	Bryan Parsons	Decision
Annual Audit Fee letter for the coming year	Grant Thornton	Discussion
Annual counter fraud report	Rob Milford	Tbc
Auditing Standards (communicating with the Audit Committee)	Grant Thornton	Decision
Prosecution Policy and Fair Processing Statements	Emma Cathcart	Decision
Whistle Blowing Policy (review)	Emma Cathcart	Decision
21 September 2016 - tbc		

Audit Committee 2014-2015 work plan

Item	Author	Decision / Discussion
11 January 2017 - tbc		
22 March 2017 - tbc		
14 June 2017 - tbc		

Items to be added at a future date (future dates will not be agreed until March 2016)		
Corporate Strategy – consideration of governance issue	Rob Milford	Tbc
Joint training session with Cotswold, West Oxford and F.O.D councillors – governance of shared services (tbc)	Rob Milford / Mark Sheldon	n/a
Policy review timetable (briefing note)	Bryan Parsons	
Requirements of the Localism Act (re: local audit)	Rob Milford	Tbc
Corporate Governance arrangements for Glos Airport following further work by the JASWG and recs arising	Mark Sheldon	Tbc
Revenue and benefits commissioning review (governance arrangements)	Mark Sheldon	Tbc
Briefing note - Audit arrangements of Airport, ICT and other services/bodies for which CBC require assurances	Rob Milford	Information
AG&M update – progress against recommendations from extraordinary meeting	Rob Milford?	Tbc
Car Parking issues – follow-up (agreed at 23/09 meeting)	Rob Milford	Tbc
Effectiveness of the Audit Committee	Rob Milford	Presentation

ANNUAL ITEMS (standing items to be added to the work plan each year)			
January	Audit committee update	Grant Thornton	Discussion
	Annual audit letter (for the previous year)	Grant Thornton	Discussion
	Certification of grants and returns (for the previous year)	Grant Thornton	Discussion
	Internal audit monitoring report (inc. counter fraud update)	Rob Milford	Discussion

Audit Committee 2014-2015 work plan

Item		Author	Decision / Discussion
	Annual governance statement – significant issues action plan	Bryan Parsons	Decision
March	Audit committee update	Grant Thornton	Discussion
	Audit plan (for the current year)	Grant Thornton	Discussion
	Auditing Standards – communicating with the Audit Committee	Grant Thornton	Decision
	Annual plan (for the upcoming year)	Rob Milford	Tbc
	Internal audit monitoring report (inc. counter fraud update)	Rob Milford	Discussion
	Annual review of risk management policy	Bryan Parsons	Decision
	Approval of the Code of Corporate Governance	Bryan Parsons	Decision
June	Audit committee update	Grant Thornton	Discussion
	Internal audit opinion (for the previous year)	Rob Milford	Discussion
	Internal audit monitoring report (inc. counter fraud update)	Rob Milford	Discussion
	Annual governance statement	Bryan Parsons	Decision
	Annual Audit Fee letter for the coming year	Grant Thornton	Discussion
	Annual counter fraud report	Rob Milford	Tbc
September	Audit committee update	Grant Thornton	Discussion
	Audit highlights memorandum - ISA 260 (for the previous year) inc. Financial Resilience	Grant Thornton	Discussion
	Internal audit monitoring report (inc. counter fraud update)	Rob Milford	Discussion
	Review of annual statement of accounts	Finance Team	Tbc

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Action	Deadline as per AGS	Action planned	Progress as at March 2016	Lead officer
To review, develop and test ICT Business Continuity Plan to ensure that it is robust enough to mitigate the identified risks for the Council and its partner organisations	March 2015	Deliver ICT Business Continuity back up arrangements through ICT shared service with FoDDC that have been tried and tested. **March 2015 position.** Business Continuity plans for the ICT Shared Service have been reviewed by South West Audit Partnership (SWAP). Senior officers from both authorities are reviewing the arrangements for individual authorities and developing a shared approach to Business Continuity. ICTSS installed and tested a back-up generator at the Coleford site this has been installed commissioned and tested. ICT SS commissioned a Disaster recovery/ Business Continuity action plan for ICTSS **Action Plan 2015/16** Close this Issue and manage within three new work streams	**Closed as per Audit Committee decision June 2015**	Director of Corporate Resources

Action	Deadline as per AGS	Action planned	Progress as at March 2016	Lead officer
Work stream 1 • Deliver effective testing of the new ICT disaster recovery (DR) plan; (ICTSS responsibility)	TBA	ICTSS to brief Audit Committee June 2015	Customer Services Manager for FoDDC and ICTSS reported to Audit committee in June that great improvement had been made and that that the ICT service had been assessed by an external company and an action plan had been put in place to further improve resilience for all of the ICTSS and Go partners. **The new 2020 partnership will include the delivery of ICT and a new ICT Business Plan will be agreed within the next 12 months.** **The 2015/16 AGS will refer to this issue with a recommendation for future reviews**	Director Resources
Work stream 2 • Ensure service area disaster recovery and business continuity plans link to the DR plan (ICTSS and CBC shared responsibility)	To follow work stream 1	Service specific Business Continuity Plans will be updated during 2015/16 to align with the Corporate Business Continuity Plan and the ICTSS Disaster Recovery Plan once the ICTSS Disaster Recovery Plan has been finalised.	All Services within CBC and external service providers are reviewing the SBCP to ensure that they can continue to deliver services in the event of an unplanned incident.	Director Resources

Action	Deadline as per AGS	Action planned	Progress as at March 2016	Lead officer
Work stream 3 • To review business continuity plans to ensure that they are robust enough to mitigate the identified service delivery risks for the Council and its partner organisations (carried forward from 2014/15) (CBC responsibility)	TBA	Consult with directors and service managers to ensure that all Service specific Business Continuity Plans are updated to align with the Corporate Business Continuity Plan and the ICTSS Disaster Recovery Plan	**This work stream will continue with the 2020 partnership once the ICT disaster recovery plan has been finalised and the Service plans have been aligned i.e. completion of work streams 1&2**	Director Resources
Safeguarding Children and Vulnerable Adults 1. Review of operational processes related to maintaining a register which identifies the training needs that relate to child protection and safeguarding for each appropriate post in the Council. 2. Hold a register of acknowledgements for all employees,	September 2015	The Learning and organisational Development Team will upload the suitable declarations to the Learning gateway and the appropriate declaration for the 'level' of training needed by each member of staff will be added to their development plans by the service manager **December position** The manager reports that the declaration process is in place and that training records are being pulled together but are not complete.	Following a report by the Partnership Team Leader, Audit Committee agreed that they had assurance that adequate and complete training records were being maintained in respect of child protection and safeguarding. They noted the fact that a section 11 self-assessment was to be undertaken and asked to be involved and to be updated on the outcome The Section 11 Audit was completed in January 2016 and submitted to the	Strategy and Engagement Manager

Action	Deadline as per AGS	Action planned	Progress as at March 2016	Lead officer
casual staff, volunteers and elected members that they have read and understood the Safeguarding Children and Vulnerable Adults handbook.		A self-assessment to comply with s11 in respect of its safeguarding practices and processes is being undertaken by the Service manager. The result of this will be considered by the Corporate Governance Group	Gloucestershire Safeguarding Children Board. We are awaiting their feedback. Feedback and the final results of the assessment will be brought to a future Audit committee meeting to allow the committee to note the results of the Council's section 11 audit and have oversight of any action recommended from the audit. **Closed as per Audit Committee decision June 2015**	

Action	Deadline as per AGS	Action planned	Progress as at March 2016	Lead officer
Car Parking An internal Audit Assurance report has identified a number of issues relating to the management of the car parking services impacting on income and operational effectiveness	September 2015	**December position** Cabinet has made budgetary provision for investment in car parking equipment, In addition, the service is reviewing the effectiveness of the Automatic Number Plate Recognition (ANPR) system in Regent Arcade car park and the experience of customers through feedback monitoring. The outcome of the review was reported to Cabinet in February 2015, with recommendations regarding any further proposed investment. **Action Plan 2015/16** Invitation to Tender documents for a Pay and Display solution for the Regent Arcade Car Park have been sent out to 5 interested companies under an ESPO Framework. Closing date for applications is 26th June. On site survey meetings will take place within this time frame as and when requested. It is hoped that replacement will take place in October/ November 2015. The Tender process for a new Pay by Phone contract has	Director of Regulatory Services provided Audit Committee with an up update report in exempt business on progress report on car parking management of the car parking services impacting on income and Operational effectiveness. **Progress was noted and the Head of Internal Audit undertook to carry out a progress report for Audit committee. Ongoing as at March 2016** **This issue will be covered in the 2015/16 AGS with a progress report.**	Head of Public Protection

Action	Deadline as per AGS	Action planned	Progress as at March 2016	Lead officer
		been completed and a new contract will be drawn up in due course.		
Purchase Order Management System compliance	September 2015	Internal Audit to undertake compliance testing of the Purchase Order management System and to report findings to Audit Committee	IA has undertaken transactional testing on the use of the Purchase Order management System across the Go Partnership. The results of these tests will be reported within the IA update report for March. It is recommended that this issue is kept open and that a follow up report is provided September 2016	Director of Resources

This page is intentionally left blank