



Notice of a meeting of Audit, Compliance and Governance Committee

Wednesday, 22 January 2020
6.00 pm
Pittville Room - Municipal Offices

| Membership | |
|---------------------|---|
| Councillors: | Steve Harvey (Chair), David Willingham (Vice-Chair), Victoria Atherstone, Matt Babbage, Jonny Brownsteen, Jo Stafford and Tony Oliver |

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 18 September 2019 | (Pages 3 - 6) |
| 4. | PUBLIC QUESTIONS These must be received no later than 12 noon on the fourth working day before the date of the meeting | |
| 5. | CYBER SECURITY UPDATE Tony Oladejo, Audit and Compliance Manager / Data Protection Officer – Business Support Services | (Pages 7 - 12) |
| 6. | AUDIT PROGRESS REPORT (Including Audit scope and additional work letter) Grant Thornton | (Pages 13 - 30) |
| 7. | INTERNAL AUDIT MONITORING REPORT Lucy Cater, Assistant Director – SWAP Internal Audit Services | (Pages 31 - 76) |
| 8. | REVISED RIPA (SURVEILLANCE AND CHIS) POLICY AND IPA (COMMUNICATIONS DATA) POLICY Emma Cathcart, Counter Fraud Manager | (Pages 77 - 128) |

| | | | |
|------------|--|--|-------------------------|
| 9. | | WORK PROGRAMME | (Pages 129 - 130) |
| 10. | | ANY OTHER ITEM THE CHAIRMAN DETERMINES TO BE URGENT AND REQUIRES A DECISION | |
| 11. | | DATE OF NEXT MEETING 24 March 2020 | |
| | | | |

Contact Officer: Saira Malin, Democracy Officer, 01242 264130
Email: democratic.services@cheltenham.gov.uk

Audit Committee

Wednesday, 18th September, 2019

6.00 - 6.35 pm

| Attendees | |
|----------------------------|---|
| Councillors: | Steve Harvey (Chair), David Willingham (Vice-Chair), Victoria Atherstone, Jonny Brownstein, Jo Stafford and Tony Oliver |
| Also in attendance: | Lucy Cater (Assistant Director of the SWAP), Emma Cathcart (Counter Fraud Manager), Paul Jones (Executive Director of Finance and Assets), Andrew Knott (Deputy Section 151 Officer) and Barrie Morris (Grant Thornton) |

Minutes

1. APOLOGIES

No apologies were received.

2. DECLARATIONS OF INTEREST

No interests were declared.

3. MINUTES OF THE LAST MEETING

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

A member asked that the minutes of item 6 (Audit Highlights memorandum ISA260) be amended to include a request for details of progress in relation to the formal lease between Ubcio and CBC in relation to recycling and refuse vehicles. This amendment was agreed.

Upon a vote it was unanimously

RESOLVED that the minutes of the meeting held on the 24 July 2019, as amended, be agreed and signed as an accurate record.

4. PUBLIC QUESTIONS

None were received.

5. INTERNAL AUDIT MONITORING REPORT

The Assistant Director of SWAP Internal Audit Services (SWAP) introduced the Internal Audit Monitoring Report, which was a quarterly report designed to give updates and assurances on the control environment and outlined progress against the 2019-20 plan. The Assistant Director highlighted that the executive summary had been amended to include details of high priority recommendations. It was also noted that since publication, the HR report had been finalised and would be summarised at the next meeting. The Executive Director of Finance and Assets advised members that the audit on Business Rates Reset had been deferred and the changes to the scheme will now not be implemented until 2021.

The Assistant Director gave the following responses to member questions:

- There were procedures in place whereby leavers email accounts were closed.
- The operational audit of 'Planning Process and Complaints Procedure' related specifically to a complaint, the audit of Planning Applications is to be undertaken later in the year.

There were no further comments or questions.

RESOLVED that the monitoring report be note.

6. COUNTER FRAUD UPDATE AND FUTURE WORK PROVISION

Emma Cathcart, Counter Fraud Manager, introduced the counter fraud update as circulated with the agenda, which provided an overview of the operational activity undertaken from the period of April 2019 to August 2019. This included: a review of empty residential properties, which supported the work of the Council's Revenues Team to manage empty properties and maximise the tax base and new homes bonus, and; areas of work with CBH which had resulted in highly successful loss avoidance. The Counter Fraud Manager also noted that a number of policies had been refreshed; the anti-fraud and corruption policy had been changed so minimally that it had simply been published on the website, but the RIPA policy had been revised completely and was currently with One Legal for comment, with a view to tabling the revised policy with the committee in January. It was unlikely that the Social Media Policy would come to the committee before April as it required a number of management decisions. For clarification she explained that a policy was in place and aimed to limit the extent to which someone could check social media accounts (i.e. Facebook pages).

The following responses were offered to Members questions:

- A request had been made that the recent 'Serious Organised Crime' seminar include assurances to members, that checklists were already in place (at the council) to identify associated risks, and she could only apologise that the session did not cover this in more detail. A review of procurement checklists was currently underway and Licensing procedures would be reviewed once this work had concluded.

Upon a vote it was unanimously

RESOLVED that the report be noted.

7. ANNUAL AUDIT LETTER

Barrie Morris introduced the Annual Audit Letter 2018-19, as circulated with the agenda. The letter summarised key findings from the work that had been undertaken for the year ended 31 March 2019, all of which had already been communicated to the committee.

A member referenced the briefing note which had been circulated with the agenda, in relation to a formal lease between CBC and Ubico. Barrie Morris confirmed that if ~~with~~ a formal lease was now in place, Grant Thornton would be

satisfied that the request had been met. This would be confirmed as part of the 2019-20 audit.

The Chairman reminded members of the request he made at the last meeting, in terms of a press release on the positive audit findings from Grant Thornton. The Executive Director of Finance and Assets confirmed that the local press had been approached about this and had not considered it newsworthy. It had however, been publicised on the website and he suggested that members may wish to use their social media platforms to publicise the matter. The Chairman was keen that the successes of the council, and by the same token, the Officers involved, be broadcast more widely and had therefore agreed to produce a briefing note for the upcoming council meeting (14 October).

The Executive Director of Finance and Assets took the opportunity to introduce Andrew Knott, the councils Deputy Section 151 Officer; as he could be called upon to cover meetings of this committee from time to time. Andrew Knott introduced himself as the Chief Accountant at Publica and explained that in his role he supported Forest of Dean as well as CBC. He assured members that he and his team had already been passed thanks for their hard work, but he would be happy to echo the comments of the committee to his team.

No decision was required.

8. WORK PROGRAMME

The work programme had been circulated with the agenda.

No amendments were raised.

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

There were no urgent items requiring a decision, however, a member queried the decision taken by Gloucestershire County Council to decarbonise their pension assets, and whether CBC could do the same and if so, what risks this would pose. The Executive Director of Finance and Assets confirmed that CBC were members of the Gloucestershire LGPS but stressed that the scheme was administered by GCC on our behalf. Therefore, any decision by GCC to decarbonise their pension assets, would benefit CBC. Whilst he couldn't say that the council had no exposure to fossil fuel investments, BP for example, he was able to confirm that the council had chosen to diversify their investments. He suggested that any member interested in knowing more about ethical investments, should attend the upcoming meeting of the Treasury Management Panel, where they were going to be considering this very issue.

A member noted that a recent article in the Financial Times had suggested that fossil fuel divestment had far less impact than investment in green technologies; seen as a positive action rather than a negative reaction.

10. DATE OF NEXT MEETING

The next meeting was scheduled for 22 January 2020.

Steve Harvey
Chairman

Cheltenham Borough Council Audit, Compliance and Governance Committee – 22 January 2020 Cyber Security Update

| | |
|---------------------------------|---|
| Accountable member | Alex Hegenbarth, Cabinet Member Corporate Services |
| Accountable officer | Tony Oladejo, Audit and Compliance Manager / Data Protection Officer |
| Ward(s) affected | All |
| Key/Significant Decision | No |
| Executive summary | To update the Audit Committee on the Cyber Security Action Plan in place, outlining the progress made against millstones to provide assurance that Cyber related risks are being managed and appropriate actions are being undertaken |
| Recommendations | That the report be noted. |

| | |
|--|---|
| Financial implications | None Contact officer: <i>paul.Jones@cheltenham.gov.uk</i> |
| Legal implications | None Contact officer: <i>Onelegal@teWKesbury.gov.uk</i> |
| HR implications (including learning and organisational development) | None Contact officer: <i>Deborah.bainbridge@publicagroup.uk</i> |
| Key risks | Failure to control and secure ICT systems and data against unauthorised access including Cyber-crime attack |
| Corporate and community plan Implications | None |
| Environmental and climate change implications | None |
| Property/Asset Implications | None Contact officer: <i>Dominic.stead@cheltenham.gov.uk</i> |

1. Executive Summary

- 1.1** In the Cyber Security update report presented to the Audit Committee in January 2019, we concluded that the ICT infrastructure is subject to ongoing and evolving cyber-attacks which, to date and to the best of our knowledge have been successfully rebuffed. It was recognised that the security infrastructure must continuously evolve to combat new threats and that the detection of Cyber incidents was as important as prevention.
- 1.2** The ICT team provides a service across 29 sites within the four Partner Councils including clients such as; Ubico, Cheltenham Borough Homes and the Cheltenham Trust serving more than 1,500 active users. Cyber & Information Security is at the forefront of all activities.
- 1.3** To enhance our resilience against a major cyber disaster, we currently adopt 'Prevent, Detect & Recover' multi-layer strategy with assurances sought for each stage. Our Cyber Security Action Plan aligns itself with the National Cyber Security Strategy. Our objective is to focus our resilience on prevention and detection activities against the threats of cyber-attacks through strengthened redesign and good preparation. By building understanding of cyber risks and threats, we can take the appropriate measures to stay safe but still take advantage of the benefits from working online.
- 1.4** As part of our ICT Business Continuity and Disaster Recovery programme to mitigate risks associated with other disaster scenarios, we continually select key disaster scenarios that may have the potential to disrupt our ICT services. This capability will be crucial in any Cyber Security incident.
- 1.5** We continually seek cyber security support and collaboration from partners such as the National Cyber Security Centre (NCSC). In a NCSC's recent Annual review 2019 , it highlighted:
- They assisted in more than 650 major cyber incidents
 - They took down more than 170,000 malicious phishing URLs sites
 - Awarded more than 14,000 Cyber Essential Certificates (including one to Cheltenham Borough Council)
- 1.6** This report outlines specific activities undertaken during 2019 aimed at improving the Cyber security arrangements for all the organisations that the ICT team support and shows the forward plan for 2020 in the tables below. The report does not include the names or the specifics of solutions used to prevent and detect Cyber incidents for obvious reasons. We are happy to share more details in person with Audit Committee members if necessary.
- 1.7** The surge in the use of Software as Service (SaaS) and our users embracing flexible working from multiple devices in a variety of locations means our traditional network perimeter is disappearing and with it, the value of traditional defences.
- 1.8** One of our key risks in 2020 will be shadow ICT through the use of unauthorised cloud based software. Whilst this is actually an Information Security risk rather than Cyber Security risk it will be seen as a Cyber incident / breach. We mitigate these risks using the Cheltenham Technical Design Authority where all requests for Applications & Systems are reviewed.
- 1.9** Over the next 12 to 24 months we see us continue to move towards a 'Zero Trust' approach to our security architecture as championed and used by the NCSC, GCHQ and other similar organisations. This is achieved by building trust into the user's identity, their devices, and the services they access rather than the networks they connect to.

Table 1 – Progress of specific Key Cyber Security Activities over 12 month period:

| Months | Key Cyber Security Activities | Status |
|---------------------------|--|------------------|
| Jan 19 to Mar 19 | <p>Cyber Essentials Plus Accreditation application process begins which includes onsite assessment by accredited security consultants.</p> <p>Changing our internal encryption cyphers (algorithms) to the latest standards to ensure compliance, in particular Payment Card Industry (PCI DSS) banking standards</p> | Completed |
| April 19 to June 19 | <p>New ICT Cyber Engineer recruited</p> <p>Internal Penetration Scan - external company (accredited Crest & Check assessors) works from within to scan all internal systems giving assurance as well as a list of vulnerabilities</p> <p>External Penetration Scan - external company attempts to break in externally and provide a report and list of vulnerabilities</p> <p>Vulnerabilities mitigated and PSN Code of Connection submitted to Cabinet Office's (PSN - Cyber Compliance Team).</p> <p>Key Milestone : Cyber Essentials Plus accreditation achieved</p> | Completed |
| July 19 to Sept 19 | <p>Key Milestone : PSN assessment completed and Certificates issued for all partner Councils</p> <p>The LGA Cyber security funding bid was successful for the Cyber Resilience awareness programme. This funding will help co-finance our Cyber security framework across the partner Councils</p> <p>Migration from Windows 2008 R2 Server (going end of life January 2020) continues.</p> | Completed |
| Oct 19 to Dec 19 | <p>All ICT staff complete additional Cyber & Data Protection awareness training.</p> <p>End user device security software changed to different supplier providing additional detection and reporting capabilities.</p> <p>Migration from Windows 2008 R2 Server (going end of life January 2020) continues.</p> | Completed |

| | | |
|--|---|--|
| | Modified infrastructure to enable compatibility with Gov Wifi enabling the rental of the 2nd Floor at the Municipal Building. | |
|--|---|--|

Table 2 - Summary of specific activities planned for 2020 (some dates may change)

| | |
|-------------------------|---|
| Jan 20 to Mar 20 | <p>Review of ICT Policies Framework – The framework consists of a number of operational Security Policies.</p> <p>Deployment of an additional network based Intrusion Detection System. (IDS)</p> <p>PSN Submission process preparation</p> <p>Mitigation put in place for Windows 2008 R2 servers not upgraded. 10 Servers in total from the 300+ servers that run on the infrastructure across all partners Councils. Extended support contract agreed by working with Crown Commercial Services as used by Central Government and the NHS.</p> |
| Apr 20 to Jun 20 | <p>Cyber Disaster recovery exercise</p> <p>Internal & External Penetration Scan work commences for annual PSN submission.</p> <p>PSN Submission</p> <p>Complete rollout of 802.1X authentication across the infrastructure.</p> |
| Jul 20 to Sept 20 | <p>Phishing Simulations exercise</p> |
| Oct 20 to Dec 20 | <p>Re-configuring on premise application servers to use the latest encryption ciphers available</p> <p>Investigate disabling weak authentication controls across the domain.</p> <p>Review service account permissions.</p> <p>Completion of online Cyber Awareness training to all CBC staff</p> |

1.10 During 2020 we will also continue to expand our cyber collaboration with external experts, these include:

- **Zephyr Regional Cyber Crime Unit**

Page 11

The partner Councils have formally recognised the Zephyr Regional Cyber Crime Unit (RCCU). This provides a forum to receive and share up-to-date cyber threat information and the sharing of best practice.

- **National Cyber Security Centre**

ICT constantly review security updates and the use of cyber support tools guidance from Central Government's National Cyber Security Centre (NCSC), their remit is to provide support to public and private sector on how to avoid cyber threats

- **Public Services Network Code of Compliance**

Public Services Network (PSN) provides an assured "network of networks" over which government and local authorities can safely share services.

2. Conclusions

- 2.1 We have an assured, secure, government-accredited security infrastructure that is able to evolve as the organisation changes.
- 2.2 People and Human Behaviour is our greatest risk. Staff awareness around Information Security and good practice when using technology should continue to be mandatory for all employees.
- 2.3 Shadow IT in the form of unauthorised Cloud based software will continue to be a risk and it is important that Managers and Staff continue to send all requests to the Technical Design Authority for approval rather than "just signing up".
- 2.4 At some point in the future, the Council will be affected by a Cyber-attack. It is sadly inevitable. However when it occurs, our detection systems will enable us to choose the best recovery method and our disaster recovery systems will allow us to recover.

| | |
|------------------------|---|
| Report author | Contact officer: Tony.oladejo@publicagroup.uk |
| Appendices | n/a |
| Background information | n/a |

This page is intentionally left blank

Audit Progress Report and Sector Update

Cheltenham Borough Council
Year ending 31 March 2020

January 2020



Contents

| Section | Page |
|-------------------------------------|------|
| Introduction | 3 |
| Progress as at January 2020 | 4 |
| Certification of claims and returns | 6 |
| Audit Deliverables | 7 |
| Sector Update | 8 |

Introduction



Barrie Morris

Engagement Lead

T 0117 305 7708
M 07771 976684
E Barrie.Morris@uk.gt.com



Aditi Chandramouli

Engagement Manager

T 0117 305 7643
M 07920 743362
E Aditi.Chandramouli@uk.gt.com

This paper provides the Audit, Compliance and Governance 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 as a local authority; and
- includes a number of challenge questions in respect of these emerging issues which the Committee may wish to consider (these are a tool to use, if helpful, rather than formal questions requiring responses for audit purposes)

Members of the Audit, Compliance and Governance Committee can find further useful material on our website, where we have a section dedicated to our work in the public sector. Here you can download copies of our publications www.grantthornton.co.uk

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 Engagement Manager.

Progress at January 2020

Financial Statements Audit

We issued our opinion on Cheltenham Borough Council's 2018/19 Statement of Accounts on 30 July 2019.

We will begin our planning for the 2019/20 audit in January and will issue a detailed audit plan, setting out our proposed approach to the audit of the Council's 2019/20 financial statements.

We will begin our interim audit in early 2020. Our interim fieldwork includes:

- Updated review of the Council's control environment
- Updated understanding of financial systems
- Review of Internal Audit reports on core financial systems
- Early work on emerging accounting issues
- Early substantive testing

We will report our work in the Audit Findings Report and provide you with regular updates on the progress of the audit

Value for Money

The scope of our work is set out in the guidance issued by the National Audit Office. The Code requires auditors to satisfy themselves that; "the Council has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources".

The guidance confirmed the overall criterion as: "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".

The three sub criteria for assessment to be able to give a conclusion overall are:

- Informed decision making
- Sustainable resource deployment
- Working with partners and other third parties

Details of our initial risk assessment to determine our approach will be included in our Audit Plan.

We will report our work in the Audit Findings Report where we will provide our Value For Money Conclusion.

The NAO is consulting on a new Code of Audit Practice from 2020 which proposes to make significant changes to Value for Money work. Please see page 10 for more details.

Progress at January 2020 (Cont.)

Other areas

Certification of claims and returns

We certify the Council's annual Housing Benefit Subsidy claim in accordance with procedures agreed with the Department for Work and Pensions. The certification work for the 2018/19 claims for Cheltenham Borough Council was completed on 26 November 2019, in advance of the 30 November 2019 deadline. We have reported our findings to the Audit, Governance and Committee further on in this report on Page 6.

We will also be finalising the certification of the pooling of housing capital receipts claim in January 2020.

Meetings

We will meet with Finance Officers in January 2020 as part of our liaison meetings and continue to be in discussions with finance staff regarding emerging developments and to ensure the audit process is smooth and effective. We will also meet with your Chief Executive regularly to discuss the Council's strategic priorities and plans.

Events

We provide a range of workshops, along with network events for members and publications to support the Council. Your officers have been invited to our Financial Reporting Workshop in February 2020, which will help to ensure that members of your Finance Team are up to date with the latest financial reporting requirements for local authority accounts.

Further details of the publications that may be of interest to the Council are set out in our Sector Update section of this report.

Audit Fees

During 2017, PSAA awarded contracts for audit for a five year period beginning on 1 April 2018. 2019/20 is the second year of that contract. Since that time, there have been a number of developments within the accounting and audit profession. Across all sectors and firms, the Financial Reporting Council (FRC) has set out its expectation of improved financial reporting from organisations and the need for auditors to demonstrate increased scepticism and challenge and to undertake additional and more robust testing.

Our work in the Local Government sector in 2018/19 has highlighted areas where financial reporting, in particular, property, plant and equipment and pensions, needs to improve. There is also an increase in the complexity of Local Government financial transactions and financial reporting. This combined with the FRC requirement that all Local Government audits are at or above the "few improvements needed" (2A) rating means that additional audit work is required.

We are currently reviewing the impact of these changes on both the cost and timing of audits. We will discuss this with your s151 Officer including any proposed variations to the Scale Fee set by PSAA Limited, before communicating fully with the Audit, Compliance and Governance Committee.

As a firm, we are absolutely committed to meeting the expectations of the FRC with regard to audit quality and local government financial reporting.

Certification of claims and returns

We completed the certification of Housing Benefit claims for Cheltenham Borough Council on 26 November 2019. Our findings are set out below:

Cheltenham Borough Council

The claim was qualified, and the following errors were noted in our report:

Cell 011 - Non HRA Rent Rebates – An error was identified in the prior year in relation to misclassification of expenditure. The full population of cell 11 was identified and the authority tested each claim. The test returned no errors and the CAKE test is considered as closed.

Cell 055 – HRA Rent Rebates – An error was identified in the prior year in relation to incorrecion calculation of earned income. As it was not possible to correctly establish the error for amendment additional testing of 40 cases was completed for the error, resulting in an extrapolated error value of £33.

Cell 055 - HRA Rent Rebates - An error was identified in our initial testing in relation to calculation of State Pension. As it was not possible to correctly establish the error for amendment additional testing of 40 cases was completed for the error, resulting in an extrapolated error value of £2,388.

Cell 055 - HRA Rent Rebates - An error was identified in our initial testing in relation to misclassification of expenditure. As it was not possible to correctly establish the error for amendment additional testing of 40 cases was completed for the error. resulting in an extrapolated error value of £627.

Cell 094 - Rent Allowances - An error was identified in our initial testing and prior year testing in relation to incorrecion calculation of earned income. As it was not possible to correctly establish the error for amendment additional testing of 40 cases was completed for the error, resulting in an extrapolated error value of £103.

Cell 094 - Rent Allowances - An error was identified in our initial testing in relation to incorrecion calculation of Occupational Pension. As it was not possible to correctly establish the error for amendment additional testing of 40 cases was completed for the error, resulting in an extrapolated error value of £13.

Audit Deliverables

| 2018/19 Deliverables | Planned Date | Status |
|--|----------------|-------------|
| Audit Findings Report The Audit Findings Report was reported to the July and November Audit, Governance and Standards Committee. | July 2019 | Complete |
| Auditors Report This is the opinion on your financial statement, annual governance statement and value for money conclusion. | July 2019 | Complete |
| Annual Audit Letter This letter communicates the key issues arising from our work. | September 2019 | Complete |
| 2019/20 Deliverables | Planned Date | Status |
| Fee Letter Confirming audit fee for 2019/20. | April 2019 | Complete |
| Accounts Audit Plan We are required to issue a detailed accounts audit plan to Audit, Compliance and Governance Committee setting out our proposed approach in order to give an opinion on the Council's 2019-20 financial statements. | March 2020 | Not yet due |
| Interim Audit Findings We will report to you the findings from our interim audit and our initial value for money risk assessment within our Progress Report. | March 2020 | Not yet due |
| Audit Findings Report The Audit Findings Report will be reported to the July Audit, Compliance and Governance Committee. | July 2020 | Not yet due |
| Auditors Report This is the opinion on your financial statement, annual governance statement and value for money conclusion. | July 2020 | Not yet due |
| Annual Audit Letter This letter communicates the key issues arising from our work. | September 2020 | Not yet due |

Sector Update

Councils continue to try to achieve greater efficiency in the delivery of public services, whilst facing the challenges to address rising demand, ongoing budget pressures and social inequality.

Our sector update provides you with an up to date summary of emerging national issues and developments to support you. We cover areas which may have an impact on your organisation, the wider local government sector and the public sector as a whole. Links are provided to the detailed report/briefing to allow you to delve further and find out more.

Our public sector team at Grant Thornton also undertake research on service and technical issues. We will bring you the latest research publications in this update. We also include areas of potential interest to start conversations within the organisation and with Audit, Compliance and Governance Committee members, as well as any accounting and regulatory updates.

- [Grant Thornton Publications](#)
- [Insights from local government sector specialists](#)
- [Reports of interest](#)
- [Accounting and regulatory updates](#)

More information can be found on our dedicated public sector and local government sections on the Grant Thornton website by clicking on the logos below:

Public Sector

Local
government

MHCLG – Independent probe into local government audit

In July, the then Communities secretary, James Brokenshire, announced the government is to examine local authority financial reporting and auditing.

At the CIPFA conference he told delegates the independent review will be headed up by Sir Tony Redmond, a former CIPFA president.

The government was “working towards improving its approach to local government oversight and support”, Brokenshire promised.

“A robust local audit system is absolutely pivotal to work on oversight, not just because it reinforces confidence in financial reporting but because it reinforces service delivery and, ultimately, our faith in local democracy,” he said.

“There are potentially far-reaching consequences when audits aren’t carried out properly and fail to detect significant problems.”

The review will look at the quality of local authority audits and whether they are highlighting when an organisation is in financial trouble early enough.

It will also look at whether the public has lost faith in auditors and whether the current audit arrangements for councils are still “fit for purpose”.

On the appointment of Redmond, CIPFA chief executive Rob Whiteman said: “Tony Redmond is uniquely placed to lead this vital review, which will be critical for determining future regulatory requirements.

“Local audit is crucial in providing assurance and accountability to the public, while helping to prevent financial and governance failure.”

He added: “This work will allow us to identify what is needed to make local audit as robust as possible, and how the audit function can meet the assurance needs, both now and in the future, of the sector as a whole.”



In the question and answer session following his speech, Brokenshire said he was not looking to bring back the Audit Commission, which appointed auditors to local bodies and was abolished in 2015. MHCLG note that auditing of local authorities was then taken over by the private, voluntary and not-for-profit sectors.

He explained he was “open minded”, but believed the Audit Commission was “of its time”.

Local authorities in England are responsible for 22% of total UK public sector expenditure so their accounts “must be of the highest level of transparency and quality”, the Ministry of Housing, Local Government and Communities said. The review will also look at how local authorities publish their annual accounts and if the financial reporting system is robust enough.

Redmond, who has also been a local authority treasurer and chief executive, is expected to report to the communities secretary with his initial recommendations in December 2019, with a final report published in March 2020. Redmond has also worked as a local government boundary commissioner and held the post of local government ombudsman.

The terms of reference focus on whether there is an “expectation gap” between the purpose of external audit and what it is currently delivering. It will examine the performance of local authority audit, judged according to the criteria of economy, effectiveness and efficiency.

Other key areas of the review include whether:

- 1) audit recommendations are effective in helping councils to improve financial management
- 2) auditors are using their reporting powers appropriately
- 3) councils are responding to auditors appropriately
- 4) Financial savings from local audit reforms have been realised
- 5) There has been an increase in audit providers
- 6) Auditors are properly responding to questions or objections by local taxpayers
- 7) Council accounts report financial performance in a way that is transparent and open to local press scrutiny

Financial Reporting Council – Summary of key developments for 2019/20 annual reports

On 30 October the Financial Reporting Council (FRC) wrote an Open Letter to Company Audit Committee Chairs. Some of the points are relevant to local authorities.

The reporting environment

The FRC notes that, “In times of uncertainty, whether created by political events, general economic conditions or operational challenges, investors look for greater transparency in corporate reports to inform their decision-making. We expect companies to consider carefully the detail provided in those areas of their reports which are exposed to heightened levels of risk; for example, descriptions of how they have approached going concern considerations, the impact of Brexit and all areas of material estimation uncertainty.” These issues equally affect local authorities, and the Statement of Accounts or Annual Report should provide readers with sufficient appropriate information on these topics.

Critical judgements and estimates

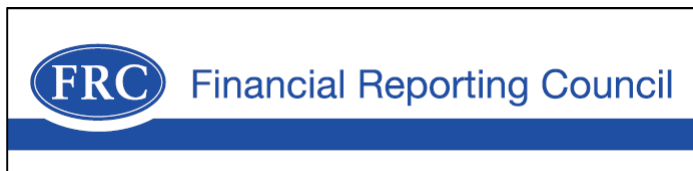
The FRC wrote “More companies this year made a clear distinction between the critical judgements they make in preparing their accounts from those that involve the making of estimates and which lead to different disclosure requirements. However, some provided insufficient disclosures to explain this area of their reporting where a particular judgement had significant impact on their reporting; for example, whether a specific investment was a joint venture or a subsidiary requiring consolidation. We will continue to have a key focus on the adequacy of disclosures supporting transparent reporting of estimation uncertainties. An understanding of their sensitivity to changing assumptions is of critical value to investors, giving them clearer insight into the possible future changes in balance sheet values and which can inform their investment decisions.” Critical judgements and estimates also form a crucial part of local authority statements of account, with the distinction often blurred.

IFRS 16 Leases

The FRC letter notes “IFRS 16 is effective for periods beginning on or after 1 January 2019. We recently conducted a thematic review looking at how companies reported on their adoption of the new standard in their June 2019 interim accounts. In advance of our detailed findings which will be published shortly, I set out what we expect to see by way of disclosures in the forthcoming accounts, drawing on the results of our work.

- Clear explanation of the key judgements made in response to the new reporting requirements;
- Effective communication of the impact on profit and loss, addressing any lack of comparability with the prior year;
- Clear identification of practical expedients used on transition and accounting policy choices; and
- Well explained reconciliation, where necessary, of operating lease commitments under IAS 17, ‘Leases’, the previous standard and lease liabilities under IFRS 16.”

The implementation of IFRS is delayed until 1 April 2020 in the public sector when it will replace IAS 17 Leases and the three interpretations that supported its application. Authorities will need information and processes in place to enable them to comply with the requirements. They will need to make disclosures in the 2019/20 accounts about the impact of IFRS 16 in accordance with IAS 8/ Code 3.3.4.3 requirements for disclosure about standards which are issued but are not yet effective.



What is the future for local audit?

Paul Dossett, Head of Local Government at Grant Thornton, has written in the Municipal Journal “Audit has been a hot topic of debate this year and local audit is no exception. With a review into the quality of local audit now ongoing, it’s critical that part of this work looks at the overarching governance and management of the audit regime. We believe there is a strong need for new oversight arrangements if the local audit regime is to remain sustainable and effective in the future.”

Paul goes on to write “Local (local authority and NHS) audit has been a key part of the oversight regime for public services for more than a century. The National Audit Office (NAO) has exercised this role in central government for several generations and their reporting to Parliament via the Public Accounts Committee is a key part of the public spending accountability framework.

Local audit got a significant boost with the creation of the Audit Commission in 1983 which provided a coordinated, high profile focus on local government and (from 1990) NHS spending and performance at a local level. Through undertaking value for money reviews and maintaining a tight focus on the generational governance challenges, such as rate capping in the 1980s and service governance failings in the 1990s, the Commission provided a robust market management function for the local audit regime. Local audit fees, appointments, scope, quality and relevant support for auditors all fell within their ambit.

However, the Commission was ultimately deemed, among other things, to be too expensive and was abolished in 2010, as part of the Coalition Government’s austerity saving plans. While the regime was not perfect, and the sector had acknowledged that reform of the Commission was needed, complete abolition was not the answer.

Since then, there has been no body with complete oversight of the local audit regime and how it interacts with local public services. The Ministry of Housing, Communities and Local Government; Department of Health; NHS; NAO; Local Government Association (LGA); Public Sector Audit Appointments Ltd (PSAA); the Financial Reporting Council (FRC); the Chartered Institute of Public Finance & Accountancy (CIPFA), audit firms and the audited bodies themselves all have an important role to play but, sometimes, the pursuit of individual organisational objectives has resulted in sub-optimal and even conflicting outcomes for the regime overall.

These various bodies have pursued separate objectives in areas such as audit fee reduction, scope of work, compliance with commercial practice, earlier reporting deadlines and mirroring commercial accounting conventions – to name just a few.

This has resulted in a regime that no stakeholder is wholly satisfied with and one that does not ensure local audit is providing a sufficiently robust and holistic oversight of public spending.

To help provide a more cohesive and co-ordinated approach within the sector, we believe that new oversight arrangements should be introduced. These would have ultimate responsibility for ensuring the sustainability of the local audit regime and that its component parts – including the Audit Code, regulation, market management and fees – interact in an optimal way. While these arrangements do not need to be another Audit Commission, we need to have a strategic approach to addressing the financial sustainability challenges facing local government and the NHS, the benchmarking of performance and the investigation of governance failings.

There are a number of possible solutions including:

- 1) The creation of a new arm’s length agency with a specific remit for overseeing and joining up local audit. It would provide a framework to ensure the sustainability of the regime, covering fees, appointments, and audit quality. The body would also help to create a consistent voice to government and relevant public sector stakeholders on key issues arising from the regime. Such a body would need its own governance structure drawn from the public sector and wider business community; and
- 2) Extending the current remit of the NAO. Give it total oversight of the local audit regime and, in effect, establish a local audit version of the NAO, with all the attendant powers exercised in respect of local audit. In this context, there would be a need to create appropriate governance for the various sectors, similar to the Public Accounts Committee.

While the detail of the new arrangements would be up for debate, it’s clear that a new type of oversight body, with ultimate responsibility for the key elements of local audit, is needed. It would help to provide much-needed cohesion across the sector and between its core stakeholders.

The online article is available here:

<https://www.themj.co.uk/What-is-the-future-for-audit/214769>

Grant Thornton's Sustainable Growth Index Report

Grant Thornton has launched the Sustainable Growth Index (formerly the Vibrant Economy Index) – now in its third year. The Sustainable Growth Index seeks to define and measure the components that create successful places. Our aim in establishing the Index was to create a tool to help frame future discussions between all interested parties, stimulate action and drive change locally. We have undergone a process of updating the data for English Local Authorities on our online, interactive tool, and have produced an updated report on what the data means. All information is available on our online hub, where you can read the new report and our regional analyses.

The Sustainable Growth Index provides an independent, data-led scorecard for each local area that provides:

- businesses with a framework to understand their local economy and the issues that will affect investment decisions both within the business and externally, a tool to support their work with local enterprise partnerships, as well as help inform their strategic purpose and CSR plans in light of their impact on the local social and economic environment
- policy-makers and place-shapers with an overview of the strengths, opportunities and challenges of individual places as well as the dynamic between different areas
- Citizens with an accessible insight into how their place is doing, so that they can contribute to shaping local discussions about what is important to them

The Index shows the 'tip of the iceberg' of data sets and analysis our public services advisory team can provide our private sector clients who are considering future locations in the UK, or wanting to understand the external drivers behind why some locations perform better than others.

Our study looks at over 50 indicators to evaluate all the facets of a place and where they excel or need to improve.

Our index is divided into six baskets. These are:

- 1 Prosperity
- 2 Dynamism and opportunity
- 3 Inclusion and equality
- 4 Health, wellbeing and happiness
- 5 Resilience and sustainability
- 6 Community trust and belonging

This year's index confirms that cities have a consistent imbalance between high scores related to prosperity, dynamism and opportunity, and low scores for health, wellbeing, happiness inclusion and equality. Disparity between the richest and poorest in these areas represents a considerable challenge for those places.

Inclusion and equality remains a challenge for both highly urban and highly rural places and coastal areas, particularly along the east coast from the North East to Essex and Kent, face the most significant challenges in relation to these measures and generally rank below average.

Creating sustainable growth matters and to achieve this national policy makers and local authorities need to do seven things:

- 1 Ensure that decisions are made on the basis of robust local evidence.
- 2 Focus on the transformational trends as well as the local enablers
- 3 Align investment decisions to support the creation of sustainable growth
- 4 Align new funding to support the creation of sustainable growth
- 5 Provide space for innovation and new approaches
- 6 Focus on place over organisation
- 7 Take a longer-term view

The online report is available here:

<https://www.grantthornton.co.uk/en/insights/sustainable-growth-index-how-does-your-place-score/>



Institute for Fiscal Studies – English local government funding: trends and challenges in 2019 and beyond

The Institute for Fiscal Studies (IFS) has found “The 2010s have been a decade of major financial change for English local government. Not only have funding levels – and hence what councils can spend on local services – fallen significantly; major reforms to the funding system have seen an increasing emphasis on using funding to provide financial incentives for development via initiatives such as the Business Rates Retention Scheme (BRRS) and the New Homes Bonus (NHB).”

The IFS goes on to report “Looking ahead, increases in council tax and additional grant funding from central government mean a boost to funding next year – but what about the longer term, especially given plans for further changes to the funding system, including an expansion of the BRRS in 2021–22?”

This report, the first of what we hope will be an annual series of reports providing an up-to-date analysis of local government, does three things in this context. First, it looks in detail at councils’ revenues and spending, focusing on the trends and choices taken over the last decade. Second, it looks at the outlook for local government funding both in the short and longer term. And third, it looks at the impact of the BRRS and NHB on different councils’ funding so far, to see whether there are lessons to guide reforms to these policies.

The report focuses on those revenue sources and spending areas over which county, district and single-tier councils exercise real control. We therefore exclude spending on police, fire and rescue, national park and education services and the revenues specifically for these services. When looking at trends over time, we also exclude spending on and revenues specifically for public health, and make some adjustments to social care spending to make figures more comparable across years. Public health was only devolved to councils in 2013–14, and the way social care spending is organised has also changed, with councils receiving a growing pot of money from the NHS to help fund services.”

The IFS reports a number of key facts and figures, including

- 1) Cuts to funding from central government have led to a 17% fall in councils’ spending on local public services since 2009–10 – equal to 23% or nearly £300 per person.
- 2) Local government has become increasingly reliant on local taxes for revenues.
- 3) Councils’ spending is increasingly focused on social care services – now 57% of all service budgets.

The IFS report is available on their website below:

<https://www.ifs.org.uk/publications/14563>





Grant Thornton

An instinct for growth™

Page 27

Paul Jones
Executive Director Finance and Assets
Cheltenham Borough Council
Municipal Offices
Promenade
Cheltenham
GL50 9SA

10 January 2019

Grant Thornton UK LLP
3rd Floor, 2 Glass Wharf
Bristol
BS2 0EL

Dear Paul

Audit scope and additional work 2019/20

In recent conversations, including at Cheltenham Borough Council's Audit Committee, we have discussed the increased regulatory focus facing all audit suppliers and the impact this will have on the scope of our work for 2019/20 and beyond. You will have also recently received a letter via email from Tony Crawley of PSAA explaining the changing regulatory landscape. In his letter, Mr Crawley highlights: *"significantly greater pressure on firms to deliver higher quality audits by requiring auditors to demonstrate greater professional scepticism when carrying out their work across all sectors – and this includes local audit. This has resulted in auditors needing to exercise greater challenge to the areas where management makes judgements or relies upon advisers, for example, in relation to estimates and related assumptions within the accounts. As a result, audit firms have updated their work programmes and reinforced their internal processes and will continue to do so to enable them to meet the current expectations."*

I promised I would set out in more detail the likely impact of this on our audit, and I am pleased to do so in this letter. Should further matters arise during the course of the audit they could also have fee and timetable implications that we would need to address at that point.

Across all suppliers and sectors (public and private), the Financial Reporting Council (FRC) has set out its expectation of improved financial reporting from organisations and the need for auditors to demonstrate increased scepticism and challenge, as well as to undertake additional and more robust testing. There is a general 'raising of the quality bar' following a number of recent, high-profile company failures that have also been attributed to audit performance. Alongside the FRC, other key stakeholders including the Department for Business, Energy and Industrial Strategy (BEIS) have expressed concern about the quality of audit work and the need for improvement. The FRC has been clear to us that it expects audit quality in local audit to meet the same standards as in the corporate world and the current level of financial risk within local audit bodies supports this position.

As a firm, we are absolutely committed to meeting the expectations of the FRC and other key stakeholders with regard to audit quality and public sector financial reporting. To ensure the increased regulatory focus and expectations are fully met, we anticipate that, as first seen in 2018/19, we will need to commit more time in discharging our statutory responsibilities, which will necessitate an increase in costs. I set out below the implications of this for your Council's audit.

Increased challenge and depth of work – raising the quality bar

The FRC has raised the threshold of what it assesses as a good quality audit. The FRC currently uses a four-point scale to describe the quality of the files it reviews, as follows:

| Score | Description |
|---------|---|
| 1 or 2a | Acceptable with Limited Improvements Required |
| 2b | Improvements required |
| 3 | Significant Improvements Required |

Historically, the FRC's definition for 2b was 'acceptable but with improvements required' and, as such, both the Audit Commission and PSAA considered a '2b' to represent an acceptance level of audit quality for contract delivery purposes. The FRC has now set a 100% target for all audits (including local audits) to achieve a '2a'. Its threshold for achieving a '2a' is challenging and failure to achieve this level is reputationally damaging for individual engagement leads and their firm. Non-achievement of the standard can result in enforcement action, including fines and disqualification, by the FRC. Inevitably, we need to increase the managerial oversight to manage this risk. In addition, you should expect the audit team to exercise even greater challenge of management in areas that are complex, significant or highly judgmental. We will be required to undertake additional work in the following areas, amongst others:

- use of specialists
- information provided by the entity (IPE)
- journals
- management review of controls
- revenue
- accounting estimates
- financial resilience and going concern
- related parties and similar areas.

As part of our planning, we have also reflected on the level of materiality which is appropriate for your audit. As outlined above, the profile of local audit has increased considerably over the past year. The reviews led by Sir John Kingman, Sir Donald Brydon and Sir Tony Redmond are focusing attention on the work of auditors everywhere. Parliament, through the work of its Scrutiny Committees, has made clear its expectations that auditors will increase the quality of their work.

As a result, you may find the audit process for 2019/20 and beyond even more challenging than previous audits. This mirrors the changes we are seeing in the commercial sectors.

Property, plant and equipment (PPE or 'Fixed Assets')

The FRC has highlighted that auditors need to improve the quality of audit challenge on Property, Plant and Equipment (PPE) valuations across the sector. We will therefore increase the volume and scope of our audit work to ensure an adequate level of audit scrutiny and challenge over the assumptions that underpin PPE valuations.

Pensions (IAS 19)

The FRC has highlighted that the quality of work by audit firms in respect of IAS 19 needs to improve across local government audits. Specifically, for the following areas, we will increase the granularity, depth and scope of coverage, with increased levels of sampling, additional levels of challenge and explanation sought, and heightened levels of documentation and reporting. Our planned additional procedures include:

- verification of the accuracy and completeness of the data provided to the actuary by both the admitted body and the administering authority.
- checking the value of the Pension Fund Assets at 31 March per the Council's financial statements against the share of assets in the Pension Fund statements
- review and assess whether the significant assumptions applied by the actuary are reasonable and are followed up on areas identified by either our review or PwC as outliers.

Page 29

- ensuring that the instructions from the audit team to the Pension Fund auditor include enquiries in respect of service organisation reports as well as testing in respect of material level 3 pension assets (please note that this is outside the scope of PSAA's fee variation process).

Complex accounting issues and new accounting standards

You are required to respond effectively to new accounting standards and we must ensure our audit work in these new areas is robust. This year we will both be responding to the introduction of IFRS16. IFRS16 requires a leased asset, previously accounted for as an operating lease off balance sheet, to be recognised as a 'right of use' asset with a corresponding liability on the balance sheet from 1 April 2020. There is a requirement, under IAS8, to disclose the expected impact of this change in accounting treatment in the 2019/20 financial statements.

We know the Council has appreciated our responsiveness in the past and we would wish to continue to be able to do this in the future.

Impact on the audit and associated costs

You will note we did not raise additional fees across the sector as a whole in 2018/19 in respect of the additional work required in response to the implementation of IFRS9 and IFRS15. This was a goodwill decision we took in support of the strong relationship we have with the sector. However, the volume of additional work now being required, as set out above, means we are no longer able to sustain that position. This is an issue not just across public services but also in the private sector where fees are being increased by all of the major suppliers by more than 20%.

We benefit from effective and constructive working relationships which we have established during our engagement with you to date. This allows us to absorb some of the impact of these changes. Using our strong working knowledge of you and efficiencies that we are continuously seeking to implement as part of our focus on continued collaborative working with you, we have sought to contain the impact as much as possible to below the market average.

We have assessed the impact of the above as follows for 2019/20, with the comparative position for the two previous years shown. Please note these are subject to approval by PSAA in line with PSAA's normal process. Should other risks arise during the course of the audit which we have not envisaged, we may need to make a further adjustment to the fee.

| Area | Cost £ | | |
|---------------------------------------|----------------|----------------|----------------|
| | 2019/20 | 2018/19 | 2017/18 |
| Scale Fee | £38,043 | £38,043 | £49,406 |
| Increased challenge and depth of work | £2,500 | - | - |
| PPE | £1,750 | £1,500 | - |
| Pensions | £1,750 | £3,000 | - |
| New standards/ developments | £1,500 | - | - |
| Total | £45,543 | £42,543 | £49,406 |

This would give a scale fee for the statutory accounts audit for 2019/20 of £38,043 plus VAT plus a variation of £7,500 plus VAT, giving a total fee of £45,543 plus VAT.

Please note that PSAA's arrangements require a separation of fees and remuneration, which means that Grant Thornton does not receive 100% of the current fees charged.

The additional work we are now planning across the whole of our portfolio will inevitably have an impact on the audit timetable and whether or not your audit can be delivered to appropriate quality standards by the 31 July 2020. Grant Thornton remains the largest trainer of CIPFA qualified accountants in the UK and is committed to continue to resource its local audits with suitably specialised and experienced staff

but the pool of such staff is relatively finite in the short-term. I will be happy to explain the impact of the further work we are planning to undertake on our delivery timetable for your audit, which at this stage is planned to be delivered by 31 July 2019.

Future changes to audit scope

As I have previously mentioned in meetings and at the audit and risk committee, the National Audit Office is currently consulting on revisions to the Code of Audit Practice and has also indicated its intention to consult on the accompanying Auditor Guidance Notes. This defines the scope of audit work in the public sector. The most significant change is in relation to the Value for Money arrangements. Rather than require auditors to focus on delivering an overall, binary, conclusion about whether or not proper arrangements were in place during the previous financial year, the draft Code requires auditors to issue a commentary on each of the criteria. This will allow auditors to tailor their commentaries to local circumstances. The Code proposes three specific criteria:

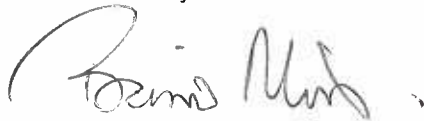
- a) Financial sustainability: how the body plans and manages its resources to ensure it can continue to deliver its services;
- b) Governance: how the body ensures that it makes informed decisions and properly manages its risks; and
- c) Improving economy, efficiency and effectiveness: how the body uses information about its costs and performance to improve the way it manages and delivers its services.

Under each of these criteria, statutory guidance will set out the procedures that auditors will need to undertake. An initial review of arrangements will consist of mandatory procedures to be undertaken at every local public body plus any local risk-based work. The consultation closed on 22 November 2019. A new Code will be laid before Parliament in April 2020 and will apply from audits of local bodies' 2020/21 financial statements onwards.

Until the consultation is finalised and more details emerge of what is expected of auditors, it is difficult to cost the impact. However, as soon as the requirements are finalised and it is clear exactly what the expectations will be, I will share with you further thoughts on the potential impact on the audit and associated costs.

I hope this is helpful and allows you to plan accordingly for the 2019/20 audit. Should you wish to discuss this further, please do not hesitate to contact me. We will be sharing our detailed Audit Plan with you in due course. We look forward to working with you again this year,

Yours sincerely



Engagement Lead and Key Audit Partner

For and on behalf of Grant Thornton UK LLP

Cheltenham Borough Council

Audit, Compliance and Governance Committee – 22 January 2020

Internal Audit Monitoring Report

| | |
|--|--|
| Accountable member | Cabinet Member Corporate Services, Councillor Alex Hegenbarth |
| Accountable officer | Paul Jones, Executive Director – Finance and Assets |
| Ward(s) affected | All |
| Key/Significant Decision | No |
| Executive summary | <p>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 SWAP Internal Audit Services (SWAP), the Council's internal audit service, is one of the control assurance sources available to the Audit, Compliance and Governance Committee, the Executive Leadership Team and Corporate Management Team and supports the work of the external auditor.</p> <p>The Annual Internal Audit Opinion presented to the Audit, Compliance and Governance 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, Compliance and Governance Committee the opportunity to comment on the work completed by the partnership and provide 'through the year' comment and assurances on the control environment.</p> |
| Recommendations | The Audit, Compliance and Governance Committee considers the monitoring report and makes comment on its content as necessary |
| Financial implications | <p>There are no financial implications arising from the report</p> <p>Contact officers: Paul Jones, Executive Director – Finance and Assets Paul.Jones@cheltenham.gov.uk, 01242 264365</p> |
| Legal implications | <p>None specific arising from the report recommendation</p> <p>Contact officer: Sarah Farooqi, Head of Law, One Legal Sarah.farooqi@tewkesbury.gov.uk, 01684 272012</p> |
| HR implications (including learning and organisational development) | <p>There are no specific HR implications arising from the content of the report. The HR Team continue to work closely with colleagues from SWAP to ensure that any HR related recommendations from audits are actioned.</p> <p>Contact officer: Julie McCarthy, HR Manager – Operations Julie.McCarthy@publicagroup.uk, 01242 264355</p> |
| 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 | <p>“Internal Auditing is 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).</p> <p>Therefore, the internal audit activity impacts on corporate and community plans.</p> |
| Environmental and climate change implications | <p>Relevant to particular audit assignments and will be identified within individual reports.</p> |
| Property/Asset Implications | <p>There are no specific Property/Asset Implications arising from the content of the report</p> <p>Contact officers: Paul Jones, Executive Director – Finance and Assets</p> <p>Paul.Jones@cheltenham.gov.uk, 01242 264365</p> |

1. Background

- 1.1 The Annual Internal Audit Plan 2019/20 was aligned with the corporate and service risks facing the Council as identified in the consultation with the Corporate Management 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 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 This report highlights the work completed by Internal Audit and provides comment on the assurances provided by this work.

3. Internal Audit Output

- 3.1 The Internal Audit Service is provided to this Council through SWAP Internal Audit Services (SWAP). SWAP is a locally authority-controlled company.
- 3.2 The SWAP report attached at **Appendix ‘A’**, sets out the work undertaken by SWAP for the Council since the Committee’s last meeting. It follows the risk-based auditing principles, and, therefore, this is an opportunity for the Committee to be aware of emerging issues which have resulted in SWAP involvement.
- 3.3 Officers from SWAP will be in attendance at the Committee meeting and will be available to address Members’ questions.

| | |
|----------------------|--|
| Report author | <div>Page 33</div> Lucy Cater, Assistant, SWAP Internal Audit Services lucy.cater@swapaudit.co.uk 01285 623340 |
| Appendices | 1. SWAP Report of Internal Audit Activity |

This page is intentionally left blank

Cheltenham Borough Council

Report of Internal Audit Activity

Plan Progress 2019/2020

January 2020

Contents

The contacts at SWAP in connection with this report are:

David Hill

Chief Executive

Tel: 01935 848540

david.hill@swapaudit.co.uk

Lucy Cater

Assistant Director

Tel: 01285 623340

lucy.cater@swapaudit.co.uk

| | | |
|---|---|--------------|
| ● | Role of Internal Audit | Page 1 |
| ● | Internal Audit Work | Page 2 |
| ● | Approved Changes to the Audit Plan | Page 3 |
| ● | Appendices: | |
| | Appendix A – Internal Audit Definitions | Page 4 – 5 |
| | Appendix B – Internal Audit Work Plan Progress | Page 6 – 11 |
| | Appendix C – Executive Summary of Finalised Audit Assignments | Page 12 – 35 |
| | Appendix D – High Priority Recommendation Follow-Up | Page 36 – 39 |
| | Appendix E – Summary of All Recommendations | Page 40 – 41 |

Internal Audit Plan Progress 2019/2020

Our audit activity is split between:

- **Governance Audit**
- **Operational Audit**
- **Key Control Audit**
- **IT Audit**
- **Other Reviews**

● Role of Internal Audit

The Internal Audit service for Cheltenham Borough Council is provided by SWAP Internal Audit Services (SWAP). SWAP is a Local Authority controlled Company. SWAP has adopted and works to the Standards of the Institute of Internal Auditors, further guided by interpretation provided by the Public Sector Internal Audit Standards (PSIAS), and also follows the CIPFA Code of Practice for Internal Audit. The Partnership is also guided by the Internal Audit Charter.

Internal Audit provides an independent and objective opinion on the Authority's control environment by evaluating its effectiveness. Primarily the work includes:

- Governance Audits
- Operational Audits
- Key Financial System Controls
- IT Audits
- Other Special or Unplanned Review

Internal Audit work is largely driven by an Annual Internal Audit Plan. This is approved by the Section 151 Officer (Executive Director – Finance and Assets), following consultation with the Council's Management Team. The 2019/20 Audit Plan was reported to, and approved by, Audit Committee at its meeting in April 2019.

Audit assignments are undertaken in accordance with this Plan to assess current levels of governance, control and risk.

Internal Audit Plan Progress 2019/2020

Outturn to Date:

We rank our recommendations on a scale of 1 to 3, with 1 being a major area of concern requiring immediate corrective action and 3 being a minor or administrative concern

● Internal Audit Work

Each completed assignment includes its respective “assurance opinion” rating together with the number and relative ranking of recommendations that have been raised with management. In such cases, the Committee can take assurance that improvement actions have been agreed with management to address these. The assurance opinion ratings have been determined in accordance with the Internal Audit “Audit Framework Definitions” as detailed in **Appendix A** of this document.

The schedule provided at **Appendix B** contains a list of all audits as agreed in the Annual Internal Audit Plan 2019/20. It is important that Members are aware of the status of all audits and that this information helps them place reliance on the work of Internal Audit and its ability to complete the plan as agreed.

As agreed with this Committee where a review has a status of ‘Final’ we will provide a summary of the work and further details to inform Members of any key issues, if any, are identified.

Further information on all the finalised reviews can be found within **Appendix C**.

At **Appendix D** we have included a schedule of the high priority recommendations (priority 1s and 2s) that have been identified during our audit reviews. These will be updated when the follow-up audit has been completed.

Appendix E summarises all recommendations made and the progress that has been made against these.

Internal Audit Plan Progress 2019/2020

We keep our audit plans under regular review to ensure that we audit the right things at the right time.

- Approved Changes to the Audit Plan

The audit plan for 2019/20 is detailed in **Appendix B**. Inevitably changes to the plan will be required during the year to reflect changing risks and ensure the audit plan remains relevant to Cheltenham Borough Council. Members will note that where necessary any changes to the plan throughout the year will have been subject to agreement with the appropriate Service Manager and the Audit Client Officer (Executive Director – Finance and Assets).

The following changes have been made to the plan:

The planned audit of Management and Monitoring of Contracts has been deferred, due to the delay in the finalising of the procurement audits. The audit, as originally planned, will be included in the 2020/21 audit plan.

At the conclusion of audit assignment work each review is awarded a “Control Assurance Definition”;

- **No Assurance**
- **Partial**
- **Reasonable**
- **Substantial**

Audit Framework Definitions

Control Assurance Definitions

| | |
|---------------------|---|
| No Assurance | The areas reviewed were found to be inadequately controlled. Risks are not well managed, and systems require the introduction or improvement of internal controls to ensure the achievement of objectives. |
| Partial | In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed, and systems require the introduction or improvement of internal controls to ensure the achievement of objectives. |
| Reasonable | Most of the areas reviewed were found to be adequately controlled. Generally, risks are well managed, but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives. |
| Substantial | The areas reviewed were found to be adequately controlled. Internal controls are in place and operating effectively and risks against the achievement of objectives are well managed. |

Non-Opinion – In addition to our opinion based work we will provide consultancy services. The “advice” offered by Internal Audit in its consultancy role may include risk analysis and evaluation, developing potential solutions to problems and providing controls assurance. Consultancy services from Internal Audit offer management the added benefit of being delivered by people with a good understanding of the overall risk, control and governance concerns and priorities of the organisation.

Recommendations are prioritised from 1 to 3 on how important they are to the service/area audited. These are not necessarily how important they are to the organisation at a corporate level.

Each audit covers key risks. For each audit a risk assessment is undertaken whereby with management risks for the review are assessed at the Corporate inherent level (the risk of exposure with no controls in place) and then once the audit is complete the Auditors assessment of the risk exposure at Corporate level after the control environment has been tested. All assessments are made against the risk appetite agreed by the SWAP Management Board.

Audit Framework Definitions

Categorisation of Recommendations

When making recommendations to Management it is important that they know how important the recommendation is to their service. There should be a clear distinction between how we evaluate the risks identified for the service but scored at a corporate level and the priority assigned to the recommendation. No timeframes have been applied to each Priority as implementation will depend on several factors; however, the definitions imply the importance.

| Categorisation of Recommendations | |
|-----------------------------------|---|
| Priority 1 | Findings that are fundamental to the integrity of the service's business processes and require the immediate attention of management. |
| Priority 2 | Important findings that need to be resolved by management |
| Priority 3 | Finding that requires attention. |

Definitions of Risk

| Risk | Reporting Implications |
|---------------|--|
| High | Issues that we consider need to be brought to the attention of both senior management and the Audit Committee. |
| Medium | Issues which should be addressed by management in their areas of responsibility. |
| Low | Issues of a minor nature or best practice where some improvement can be made. |

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|------------------------|-------------------------------------|---------|--------------------|------------|-----------|---|---|---|-------------------------------|
| | | | | | | 1 | 2 | 3 | |
| | | | | | | 2018/19 Audits in Draft / In Progress at Annual Opinion | | | |
| Operational | Procurement and Contract Management | | Final Report | Reasonable | 1 | | 1 | | See Appendices C & E |
| Key Financial Control | Systems Admin | | Final Report | Reasonable | 7 | | 2 | 5 | Reported at September Meeting |
| Key Financial Control | Human Resources | | Final Report | Reasonable | 2 | | 1 | 1 | See Appendices C & E |
| Key Financial Control | Procurement | | Final Report | Partial | 10 | | 7 | 3 | See Appendices C & E |
| ICT | Cyber Security | | Draft Report | | | | | | |
| Operational | Integrity of Data | | Draft Report | | | | | | |
| Advice and Consultancy | Benefits Realisation | | Position Statement | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Internal Audit Work Plan Progress 2019/2020

APPENDIX B

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|--------------------|--|---------|---------------|-------------|-----------|----------|---|---|-------------------------------|
| | | | | | | 1 | 2 | 3 | |
| 2019/20 Audit Plan | | | | | | | | | |
| Governance | Annual Governance Statement | 1 | Final Report | Substantial | 2 | | | 2 | See Appendices C & E |
| Operational | Management and Monitoring of Contracts | 1 | Deferred | | | | | | |
| Operational | Asset Management | 1 | In Progress | | | | | | |
| Operational | Commercial Property / Investment Property | 1 | In Progress | | | | | | |
| Operational | Safeguarding | 1 | In Progress | | | | | | |
| Operational | Remote Workers | 1 | Final Report | Substantial | 2 | | | 2 | See Appendices C & E |
| Operational | Commissioning (2018/19) | 1 | Audit Removed | | | | | | |
| ICT | Software as a Service – Cloud Provision | 1 | ToE Issued | | | | | | |
| ICT | Software as a Service – Dataset Management | 1 | ToE Issued | | | | | | |
| Follow-Up | Ubico Financials | 1 | Final Report | Substantial | 1 | | | 1 | Reported at September Meeting |
| Follow-Up | Business Continuity Management | 1 | In Progress | | | | | | |
| Operational | (NEW) Property (Use of Contractors) | 1 | Final Report | Partial | 5 | | 5 | | See Appendices C & E |
| | | | | | | | | | |

Internal Audit Work Plan Progress 2019/2020

APPENDIX B

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|-----------------------|--|---------|--------------|-------------|-----------|----------|---|---|----------------------|
| | | | | | | 1 | 2 | 3 | |
| Operational | Affordable Housing | 2 | In Progress | | | | | | |
| Operational | Business Rates Reset | 2 | Deferred | | | | | | |
| Operational | Apprenticeship Scheme | 2 | Final Report | Substantial | 1 | | 1 | | See Appendices C & E |
| ICT | Cyber Security – Incident Management | 2 | ToE Issued | | | | | | |
| ICT | Cyber Security – High Risk Area (defined from 2018/19 audit) | 2 | | | | | | | |
| Grant Certification | Disabled Facilities Grant Certification | 2 | Complete | | | | | | |
| Operational | (NEW) Planning Process and Complaints Procedure | 2 | In Progress | | | | | | |
| | | | | | | | | | |
| Key Financial Control | Revenues and Benefits | 3 | | | | | | | |
| | • National Non-Domestic Rates | | Final Report | Substantial | 1 | | | 1 | See Appendices C & E |
| | • Council Tax | | | | | | | | |
| | • Council Tax Benefit | | Final Report | Substantial | 0 | | | | See Appendix C |
| Key Financial Control | Core Financials | 3 | | | | | | | |
| | • Accounts Payable | | Final Report | Substantial | 0 | | | | See Appendix C |

Internal Audit Work Plan Progress 2019/2020

APPENDIX B

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|-----------------------|--|---------|--------------|------------|-----------|----------|---|---|----------------------|
| | | | | | | 1 | 2 | 3 | |
| | • Accounts Receivable | | In Progress | | | | | | |
| | • Main Accounting | | | | | | | | |
| | • Payroll | | In Progress | | | | | | |
| | • Treasury Management and Bank Reconciliation | | | | | | | | |
| Key Financial Control | Systems Administration | 3 | In Progress | | | | | | |
| Key Financial Control | Human Resources – Use of Volunteers | 3 | Final Report | Reasonable | 7 | | 3 | 4 | See Appendices C & E |
| Key Financial Control | Other Support Service provided by Publica • Health and Safety | 3 | In Progress | | | | | | |
| ICT | Management of Service Provision | 3 | | | | | | | |
| ICT | ICT Business Continuity | 3 | In Progress | | | | | | |
| Grant Certification | Disabled Facilities Grant Certification – Additional Grant | 3 | Complete | | | | | | |
| | | | | | | | | | |
| Governance | Risk Management | 4 | | | | | | | |
| Governance | Performance Management | 4 | | | | | | | |
| Operational | Planning Applications | 4 | | | | | | | |

Internal Audit Work Plan Progress 2019/2020

APPENDIX B

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|------------------------|---|---------|----------|---------|-----------|----------|---|---|----------|
| | | | | | | 1 | 2 | 3 | |
| Operational | Publica Transformation Benefits Realisation | 4 | | | | | | | |
| Operational | Corporate Culture | 4 | | | | | | | |
| | | | | | | | | | |
| Follow-Up | Follow-Up of Recommendations made in Substantial and Reasonable Audits | 1 – 4 | On Going | | | | | | |
| Follow-Up | Follow-Up of Control Weaknesses identified by the Counter Fraud Unit | 3 – 4 | On Going | | | | | | |
| | | | | | | | | | |
| Advice and Consultancy | Workforce Strategy | 1 – 4 | | | | | | | |
| Advice and Consultancy | Support to the Publica Transformation Programme | 1 – 4 | On Going | | | | | | |
| Advice and Consultancy | Assurance to the Partner Councils in respect of the Publica Transformation Programme | 1 – 4 | | | | | | | |
| Advice and Consultancy | Support for any emerging groups / programmes / projects • Town Centre Team Project Board | 1 – 4 | On Going | | | | | | |

Internal Audit Work Plan Progress 2019/2020

APPENDIX B

Internal Audit Work Plan Progress 2019/2020

APPENDIX B

[illegible]

Audit Assignments finalised since the last Audit Committee:

● Summary of Audit Findings and High Priority Service Findings

The following information provides a brief summary of each audit review finalised since the last Committee update.

2018/19 – Procurement and Contract Management – Reasonable Assurance

Background

The Publica Procurement Service provides a collaborative approach to procurement work, information and guidance to the Publica partner Councils – Cheltenham Borough Council (CBC), Cotswold District Council (CDC), Forest of Dean District Council (FoDDC) and West Oxfordshire District Council (WODC) as well as Ubico and Cheltenham Borough Homes (CBH). The objective of the service is to improve the way the Council and partners procure services, goods and works, and manage contracts to deliver improved quality services and make sure public spending is achieving value for money.

Contracts and relationship management refers to the effective management and control of all contracts from their planned inception until their completion by the appointed contractor(s). It covers the supporting policies, procedures and systems needed to undertake it, together with broader issues from the identification and minimisation of risk, successful and timely delivery of outcomes and performance, effective control of cost and variations and the maintenance of clear communications and operational relationships with contractors. Once a contract is in place, contract management is the responsibility of the contract owner or another delegated contract manager.

The Procurement and Contract Management Strategy sets out contract management guidance and requirements. The In-Tend Portal can be used by contract managers to prompt contract management activities, with an enhanced Contract Management Wizard module in the process of being purchased and set up as an add-on to the In-Tend Portal.

Audit Conclusion / Findings

Procurement Services are provided to Cheltenham Borough Council (CBC) by Publica Group Ltd (Publica).

Evidence was found to confirm some sound procurement and due diligence processes during the tender stages. Relevant evidence and information is requested of potential suppliers at various stages, including as part of pre-procurement considerations and tender questionnaires. Proportionate and adequate supplier checks are made by

Procurement Officers in line with the value and nature of the prospective contract.

Although there is a Procurement and Contract Strategy in place for the Partner Councils, it is out of date and in need of review and update. Tools are available to contract owners through the In-Tend Procurement Portal to monitor and manage contracts. However, training to encourage use of contract management modules on the portal has been delayed due to limited staffing resource within the Procurement Team.

According to the National Procurement Strategy 2018, research by the International Association for Contract and Commercial Management (IACCM) shows that contracts exceed their expected costs by 9.4 per cent on average over their lifetime. Poor contractor performance could seriously damage the Council's reputation and its ability to deliver effective services and support to local communities. The absence of ongoing due diligence and contract management by contract owners throughout the life of the contract could expose the Council to unnecessary risk in multiple areas, such as financial, legal, compliance and operational risk.

Following on from this governance review, we will conduct a further audit on Management and Monitoring of Contracts undertaken by CBC officers as part of the 2019/20 Audit Plan.

| Priority | Recommendation | Management Response | Due Date |
|----------|--|---------------------|----------------------------|
| 2 | Assurance is sought from Publica that the Procurement and Contract Management Strategy is reviewed and updated to ensure it meets the needs of Publica and the partner Councils. | Agreed | 30 th June 2020 |

2018/19 – Human Resources (Sickness Absence Reporting) – Reasonable Assurance

Background

HR and Payroll services are a centralised function provided by Publica Group (Support) Ltd (Publica), a Council owned company to the four partner Councils Cotswold District Council (CDC), West Oxfordshire District Council (WODC), Forest of Dean District Council (FoDDC) and Cheltenham Borough Council (CBC), as well as, Ubico Ltd, Cheltenham Borough Homes (CBH) and the Cheltenham Trust.

Payroll related processes including sickness recording are currently manual at CBC although a Self-Service functionality is available on Agresso Business World (ABW).

Testing samples were taken from ABW from the following date range: 1st November 2017 – 31st October 2018. During this time, the sickness absence recorded for CBC was 1599 FTE days.

Audit Conclusion / Findings

We are pleased to offer reasonable assurance over the following processes within the HR and Payroll Service:

- Existence of Sickness Policies.
- Appropriate action following periods of sickness absence.
- Sickness absence payment and calculations.
- Sickness payments accuracy checks.

No significant risks were identified during the review, although there are areas where there is opportunity for improvement. These areas are highlighted within the report and recommendations made to improve processes have been made in the areas as described below.

At the time of the review there was no approved Sickness Absence Policy for Publica employees, including new employees. Sickness absence policies exist for all four of the Member Councils; however, it was noted that they had not been reviewed and updated recently. This has therefore highlighted the need for timely implementation of a Publica Sickness Policy, so there are clear and consistent guidelines in place for all staff. Council sickness absence policies should also be reviewed and updated, to ensure they are still in line with relevant legislation and are appropriate to the officers retained by the Councils.

Line managers are responsible for monitoring and the reporting of sickness absence to Payroll, Cheltenham Borough Council (CBC) do not utilise self-service, so reporting to payroll is completed monthly via a manual form. Managers are also responsible for holding a return to work interview, completing a form to be signed by both employee and manager to be returned to HR for checking and filing. Testing found that not all forms were found on file or fully completed, and we have therefore recommended refresher training and guidance is provided following the review and update of relevant Sickness Policies.

Controls are in place for Payroll Advisors to monitor long-term sickness absence, ensuring any amendments to pay are

made in accordance with terms and conditions are captured and actioned at the correct time. Different methods are used across the team during this process; therefore, we recommend standardising the process for consistency.

Sickness variation reports are produced from the Business World System and checked by Payroll Officers during each payroll run. The checking of these reports highlights if there is a discrepancy in pay caused by a system anomaly and enables personnel to correct the anomaly to ensure the correct payment prior to payroll authorisation and release.

| Priority | Recommendation | Management Response | Due Date |
|----------|---|--|--------------------------------|
| 2 | We recommend that the Publica Sickness and Absence Policy is finalised, approved and implemented without delay. The partner councils' Sickness and Absence Policies should also be reviewed and updated to ensure they meet the ongoing needs of the Councils and their retained staff. | The Policy is now complete and will be rolled out to managers after the summer break 2019. We will review the council policies. These will be brought in line with the new Publica policy if and when the partner Councils adopt the new Publica terms and conditions. | 30 th November 2019 |

2019/20 – Remote Workers – Substantial Assurance

Background

The Council currently has 28 lone workers managed by the following service managers:

- Head of Revenues & Benefits
- Customer & Support Services Manager
- Strategy & Engagement Manager
- Enforcement Manager
- Parking Administrator/Business Support Manager

The Enforcement team is the largest with 16 members of staff lone working on a regular basis. Other officers working in service areas such as Building Control, Planning, Licensing, etc, may on occasion lone work but generally, their appointments are made in advance and are shown in Outlook calendars, therefore colleagues based at the office know of their whereabouts. They are not included in the above figure.

The Council's Modernisation programme is encouraging officers to 'Smart Work' which means that work can be completed at a time and place to suit the individual providing the necessary ICT equipment and health and safety systems are in place. Therefore, the likelihood of more officers potentially lone working will significantly increase thereby increasing the need to have appropriate processes in place.

Audit Conclusion / Findings

Lone Working H&S Arrangements

The Council has an up to date Lone Working Policy in place which is easily accessible on the staff intranet. Review of the policy confirms that relevant Health & Safety (H&S) legislation is referenced, roles and responsibilities are clearly identified and guidance on local arrangements is provided.

To test compliance with the Lone Working Policy, we interviewed 5 service managers and can confirm that appropriate processes are in place for the officers, who are lone workers, in these areas. Officers are trained and provided with council mobile phones so that contact is always maintained. Service specific systems are in place to monitor when lone workers start and finish their working day.

We can also confirm that CBC canvassers, working on behalf of Elections, must attend training/briefing sessions where H&S is discussed, and a Canvassers Manual is provided which contains detail in respect of H&S when undertaking their duties.

There is no corporate personal safety system in place for lone workers, therefore the information on the intranet is out of date. We can confirm that 2 service managers are exploring systems that would suit their service needs, however, there is a risk that different systems could be implemented which may result in savings from economies of scale not being achieved. Therefore, a corporate approach would mitigate this risk and ensure that an effective system is implemented in a timely manner. We were also advised that the Personal Safety Register, which is a register of potentially dangerous individuals was being reviewed to ensure that it was still fit for purpose and to ensure that it does not breach any data protection regulations.

Smart Working Policy

With the Modernisation Programme gaining pace, we were asked to review the draft Smart Working Policy that is currently being developed by the Publica HR team. We have made several observations/suggestions for consideration

which are detailed in the body of this report. It is important that the Policy and accompanying procedure/guidance documents are agreed and made available as soon as possible so that officers are aware of their roles and responsibilities and management expectations in terms of working practices.

Finally, we noted that some remote working information on the intranet is either obsolete or in need of updating. When the Smart Working Policy is agreed the intranet should be reviewed and updated with relevant up to date information.

2019/20 – Property (Use of Contractors) – Partial Assurance

Background

Following the 2018/19 audit of Accounts Payable and as part of good governance and commitment to financial transparency we were instructed to undertake a review of the Property Services Department.

The Cheltenham Borough Council (CBC) Property Services Department manage the planned and reactive maintenance requirements of the Cheltenham Borough Council property portfolio, including but not limited to the Municipal Offices, Cheltenham Town Hall, Pittville Pump Rooms and the town's leisure centre. Many of the properties are listed buildings and require specialist care and attention.

Property Services have annual budgets for reactive, planned and cyclical maintenance and programme works. Annual programmes of work are prioritised, presented to and then approved by Council.

Properties are maintained by engaging external property maintenance providers, depending on the works required. An approved contractor framework exists so that services can be obtained on the basis of pre-agreed terms and conditions, price and quality levels. The contractor framework consists of three contractors. CBC were also authorised to use the Gloucestershire County Council Contractor Framework until its renewal in April 2019.

Analysis of Property Services expenditure (incl. vat) to those contractors can be seen in the following table which includes planned and responsive works to July 2019.

| Contractor | 2016/17 | 2017/18 | 2018/19 | 2019/20 | Totals |
|--------------|---------|----------|----------|---------|----------|
| Contractor A | £0 | £40,441 | £14,434 | £3,142 | £54,875 |
| Contractor B | £23,771 | £260,605 | £53,340 | £5,106 | £342,822 |
| Contractor C | £0 | £44,596 | £131,184 | £33,961 | £209,741 |
| Contractor D | £36,331 | £93,532 | £105,663 | £8,645 | £244,171 |

It was identified that Contractor D was not on the framework, although we can confirm this is being addressed appropriately.

Audit Conclusion / Findings

Our review focussed on the following three process areas within Property Services.

Use of the Council's Contractor Framework

We were advised by the Senior Surveyor that the Council's current contractor framework, whilst in date, was not very effective with only three contractors on it. The Gloucestershire County Council (GCC) framework was also available for use until its renewal in April 2019. The officer explained that he has been working with the Procurement and Legal teams to get the contractor framework updated for at least two years and various issues have delayed progress on this work, which has resulted in non-compliance with the Council's Financial and Contract Rules.

How works are identified, costed and approved

Whilst we can confirm processes are operating to identify and approve works, they are not as robust as expected. There is a lack of transparency and audit trails are not always available. We recognise that responsive repairs need to be completed as soon as possible and therefore could lead to added pressures however, works must be awarded appropriately and in accordance with agreed procedures.

The awarding and payment of works

Our review found that it is not clear how responsive maintenance works are awarded to contractors. As discussed above there is a contractor framework, which is not always used, and the lack of audit trails has meant that we are unable to confirm if appropriate processes are undertaken.

Our testing identified that some contractor invoices contained limited detail as to the works undertaken, including itemisation between materials and labour, and have been authorised and paid without this detail. In addition, budget

monitoring processes were not sound, however, we can confirm steps are being taken to improve this area.

In summary, a lack of guidance and procedures has resulted in inconsistent processes operating which has led to a lack of transparency over decisions taken and has the potential of allegations being made of works being awarded inappropriately. Recommendations made in this report should be implemented urgently to improve the control environment.

An end to end process review has not been possible due to the control weaknesses identified, therefore we will undertake a further review in next year's audit plan to cover this area in more detail.

| Priority | Recommendation | Management Response | Due Date |
|----------|---|---|-----------------------------|
| 2 | <p>We recommend:</p> <p>i. that unless specialist skills are required to complete specific works, only approved framework contractors are used for general building works.</p> <p>ii. that the progress of updating the contractor framework is pursued and if necessary escalated through Publica/One Legal Client Officers and Senior Management to ensure focus on this requirement is maintained.</p> | <p>Now using only framework contractors or obtaining waivers for non-specialist works.</p> <p>Additional frameworks are being pursued through One Legal for use of the GCC framework and Publica Procurement for additional frameworks.</p> | 31 st March 2020 |

| | | | |
|---|--|---|-----------------------------|
| 2 | <p>We recommend</p> <p>i. that process documents and associated procedures, aligned with CBC's Contract and Financial Rules, are documented and put in place so that a consistent approach to tasks can be followed and undertaken within the team as soon as possible.</p> <p>ii. A review of the service design should be undertaken to ensure that appropriate and effective processes and structures are in place.</p> | <p>Develop flow charts and sub processes to be agreed and signed off by section 151 officer.</p> <p>Started and talked already with Director and Publica Procurement to produce report on options going forward for strategic procurement of building related needs.</p> | 31 st March 2020 |
| 2 | <p>We recommend</p> <p>i. that the frequency of budget monitoring and reconciliation between the Council's financial system and the Uniform system is undertaken in accordance with the Financial Rules so that any issues related to budgets and expenditure are identified at an early stage. Regular management information reporting should be implemented to ensure transparency of the situation.</p> <p>ii. Consideration should be given to investigating whether the Uniform and Business World systems can be linked to aid budget monitoring processes.</p> | <p>Publica Finance has now appointed an accountant to liaise with and we will reconcile the Uniform and Agresso figures quarterly. Reviews are set up to feed into the financial reporting cycle.</p> <p>A brainstorming session has been set up to review the way Uniform and Agresso are used and explore what functionality and data can to be shared across systems. Once this is determined, we will liaise with Publica IT to progress further.</p> | 31 st March 2020 |

| | | | |
|---|--|--|---|
| 2 | We recommend that the Property Services team, return any invoice that does not contain detailed information on the works completed, including materials and labour costs and ensure only sufficiently detailed invoices are approved for payment. | We have contacted the contractors and requested that a breakdown of invoices are provided in all cases. All staff have been instructed to return invoice if they are not adequately broken down. | 31 st March 2020 |
| 2 | To protect the separation of duties between requisitioning and approval of works, we recommend that in urgent circumstances where this is necessary a clarification email is sent to the Head of Property and Assets to confirm the actions taken. | Implemented already. The Senior Surveyor is not raising work orders except in emergencies wherein an email is sent to the Head of Service, so he is aware of the action being undertaken. | Recommendation Actioned and therefore can be closed |

2019/20 – Apprenticeship Scheme – Substantial Assurance

Background

The Apprenticeship Levy was introduced in April 2017 and is a levy on UK employers to fund new apprenticeships. The levy applies to employers with an annual pay bill of over £3 million and is charged at 0.5% of the employer's annual pay bill. Each employer is given an allowance of £15,000 to offset against their levy payment. The Apprenticeship Levy is charged annually but employers report and pay it monthly through Pay As You Earn (PAYE), and the monthly calculation is based on the total pay bill for the tax month.

In England, control of apprenticeship funding is given to employers through the Digital Apprenticeship Service (DAS). The DAS allows employers to receive levy funds, manage apprentices and choose and pay training providers. Apprenticeship Levy funds can be used to upskill current employees as well as recruiting new employees on apprenticeships.

Based on its current annual pay bill, Cheltenham Borough Council (CBC) pays between £1500 and £1600 as a levy payment each month. As of September 2019, CBC employed 9 apprentices with 2 new positions in the process of being filled. There were also 2 existing employees benefiting from upskilling using the Apprenticeship Levy, with 5 new

opportunities pending. It is a Government requirement that “prescribed groups and public sector bodies with 250 or more staff in England have a target to employ an average of at least 2.3% of their staff as new apprentice starts over the period of 1 April 2017 to 31 March 2021. Based on the information provided during the audit, this target is currently being met.

Audit Conclusion / Findings

Processes surrounding the recruitment and training of apprentices are robust and well-established. We are able to confirm that procurement of apprenticeship training is in line with Government requirements and providers are subject to a thorough process which ensures value for money and quality of training. Key officers are in place from recruitment of an apprentice through to ongoing mentoring in service areas.

Apprenticeship Levy payments are calculated using an automated report on Agresso Business World (ABW) by the Payroll Team Leader, who is experienced in her role. Testing concluded that payments were correctly calculated, recorded and paid through PAYE. We were able to reconcile the payments to the online Digital Apprenticeship Service (DAS), through which the HR Talent Development Business Partner can pay apprenticeship training providers using levy funds. It was identified during the audit, however, that reconciliation is not carried out by the service area. A recommendation has been made to implement a reconciliation process which will mitigate any possible financial risk.

| Priority | Recommendation | Management Response | Due Date |
|----------|---|---|--|
| 2 | We recommend that a reconciliation process is implemented for Apprenticeship Levy payments. | Reconciliation is now carried out monthly between the Finance spreadsheet, the General Ledger and the online apprenticeship levy portal. Support will be requested from Finance to ensure reconciliation is being done correctly in the initial stages. The internal apprentice recruitment form has also been amended to ensure that the recruiting manager consults with the Finance Department to ensure there is appropriate levy funding available in the online account before the post goes for approval at the | Implemented & ongoing (to be followed up Feb 2020) |

| | | | |
|--|--|--------------------------|--|
| | | Resource Managers Group. | |
|--|--|--------------------------|--|

2019/20 – Revenues and Benefits (Council Tax and National Non-Domestic Rates) – Substantial Assurance

Background

The Revenues and Benefits service area are responsible for the day to day processing, collection and arrears management, and application of any discounts and reliefs of Council Tax and NNDR as well as Housing Benefit and Council Tax support schemes.

Council Tax is a local property tax to help fund local public services and is payable on all residential properties regardless of whether they are rented or owned. Discounts and exemptions are available under certain circumstances, including but not limited to discounts for students, single person occupation and unoccupied properties.

NNDR is also a tax collected to contribute towards the cost of local services and is payable on non-domestic properties. Reliefs and discounts are available under certain circumstances, including unoccupied or partly occupied properties, small business rate relief and charity occupied properties.

The Revenues and Benefits service area constantly handle personal information and are therefore required to comply with the regulations set out in the Data Protection Act 2018 which incorporates the General Data Protection Regulations (GDPR).

Audit Conclusion / Findings

Council Tax and National Non-Domestic Rates (NNDR) discounts and exemptions can be applied to accounts in certain circumstances. Testing found that where this is applicable, evidence and appropriate notes to support the discounts given were documented in the Council Tax and NNDR system. Ongoing discounts and exemptions are reported and reviewed periodically.

The Council Tax and NNDR systems are reconciled to the General Ledger approximately twice per month. Daily checks of the cash receipt load files into the Council Tax and NNDR system are undertaken. Testing confirmed these reconciliations are completed accurately and checked by an independent Officer. As part of the annual billing process, reconciliation of the Council Tax and NNDR bills issued by the mailing companies to that expected on the Council Tax and NNDR system is undertaken which ensures bills are issued as required.

Exception reports for areas including arrears, credits and suppressed accounts are regularly run and found to be actioned appropriately. The suspense accounts are checked and actioned on a daily basis by a Revenues Officer working with a Finance Officer to correctly re-allocate funds.

Monthly Management Information is produced and reviewed/discussed with the Head of Revenues & Benefits, and then cascaded to the rest of the team ensuring awareness of the service area's overall work status against targets.

Business Continuity Plans (BCP) are documented, have been reviewed and updated during this year and are in place for staff should they need to be instigated.

Data Protection (GDPR) education has been provided to the Revenues and Benefits staff, and processes are in place to ensure compliance with these regulations.

2019/20 – Revenues and Benefits (Housing Benefit and Council Tax Support) – Substantial Assurance

Background

The Revenues and Benefits service area are responsible for the day to day processing, collection and arrears management and application of any discounts and reliefs of Council Tax and NNDR as well as Housing Benefit and Council Tax support schemes.

Housing Benefit is a means-tested benefit which is administered on behalf of the Department of Works and Pensions (DWP). New claimants who meet the criteria for Universal Credit or existing recipients of Universal Credit are not able to claim Housing Benefit.

Local authorities are entitled to make an annual claim for the refund of the housing benefit subsidy from Central Government. The claim should be submitted by 30th April and it is then required to be independently audited by 30th

November each year.

Cheltenham Borough Council implemented a new Council Tax Support scheme from the year 2019/20. Council tax support helps people on low income to pay their council tax. The scheme is approved locally for working age customers and nationally for pension age customers.

The Revenues and Benefits service area constantly handle personal information and are therefore required to comply with the regulations set out in the Data Protection Act 2018 which incorporates the General Data Protection Regulations (GDPR).

Audit Conclusion / Findings

Reconciliations for Housing Benefits payments to the General Ledger are undertaken approximately twice per month by a Revenues and Benefits Officer. Testing identified that these are completed accurately and are routinely checked by an independent Officer.

We can confirm that claims processing is monitored via a performance report and evidence showed that processing targets were consistently met. Quality checking is performed by the Benefits Team Leader on at least 10% of all claims. Testing showed that 'critical' or 'non-critical' errors are recorded in monitoring control sheets and fed-back to the Officer concerned for correction. We note that the definitions of 'critical' and 'non-critical' errors were defined over twenty years ago and that sample checking is primarily a manual paper-based process. Although a formal recommendation is not being made, we would suggest that consideration could be given to reviewing current practices to aid efficiencies and reduce any potential data protection or document retention issues.

Monthly Management Information is produced and reviewed/discussed with the Head of Revenues & Benefits, and then cascaded to the rest of the team ensuring awareness of the service area's overall work status against targets.

The Subsidy Claim process is managed by the Deputy Revenues & Benefits Manager. Evidence of monthly reconciliations and Civica reports were seen to support the monitoring that is undertaken to provide an estimate for the year end claim. Following the External Auditor's 2017/18 qualified audit report the Deputy Revenues and Benefits Manager advised that additional controls have been introduced to prevent issues in the future.

Business Continuity Plans (BCP) are documented, have been reviewed and updated during this year and are in place for

staff should they need to be instigated.

Data Protection (GDPR) education has been provided to the Revenues and Benefits staff, and processes are in place to ensure compliance with these regulations.

Finally, we can confirm that the two recommendations from the 2018/19 audit have been implemented.

2019/20 – Accounts Payable – Substantial Assurance

Background

As part of the 2019/20 Internal Audit plan, a review was carried out to provide our partners and clients assurance over the adequacy of procedures and controls in place within the Accounts Payable department.

Accounts Payable (based at Forest of Dean District Council) is a centralised function that processes invoices, payment requests and feeder payments, such as Accounts Receivable refunds and benefit payments, on behalf of the following clients:

- G1- Cheltenham Borough Council (CBC)
- G2- Forest of Dean District Council (FoDDC)
- G3- West Oxfordshire District Council (WODC)
- G4- Cotswold District Council (CDC)
- G5- Cheltenham Borough Homes (CBH)
- G6- Ubico
- G7- The Cheltenham Trust
- P8- Publica

All payments are processed using the financial management system: Business World. All invoices for goods and services go to FoDDC, either directly from the supplier or forwarded by service areas. Invoices are scanned and saved within the Business World transaction file. Where purchase orders have been raised by the service area, invoices can be matched to these, and assuming the goods have been receipted, payment can be made immediately. Where no purchase order has been raised the details from the invoice are entered manually into Business World. Officers within the service area that received the goods/services with appropriate approval rights are required to review the payment details and approve the payment or reject it if they require any of the payment details changing (i.e. the payment cost centre or account). Payment runs are created weekly, which are sense checked by the AP Team Leader and authorised by the

Business Partner Accountant (this process was reviewed as part of last year's audit).

Our review used payments processed between September 2018 and September 2019 on behalf of CBC. The number and value of these payments, have been compared to the same period in the previous year and shown below:

| | | 2018/19 | | 2019/20 | |
|----|-----|---------|-------------|---------|-------------|
| | | Number | Value | Number | Value |
| G1 | CBC | 8371 | £49,956,277 | 8553 | £46,705,210 |

Audit Conclusion / Findings

We are pleased to offer Substantial Assurance over the following procedures within Accounts Payable:

- Processing invoices to ensure debts are paid by the appropriate client
- Duplicate payments are identified and recovered timely
- Limiting the use of Sundry Supplier payments
- Preventing fraudulent payments

Testing was carried out to identify outstanding duplicate payments. In all cases where duplicate payments were still outstanding the Accounts Payable Team Leader provided evidence that these payments were in the process of being recovered. We also carried out testing to ensure the service's processes around limiting the use of Sundry Supplier payments were being followed. We did not find any instances that the process described within the report was not being followed. Finally, we tested all payments made within our test period to the bank details of employees of the Councils, Publica and CBH. No fraudulent payments were identified as part of this testing.

2019/20 – Human Resources (Use of Volunteers) – Reasonable Assurance

Background

As a Local Authority, Cheltenham Borough Council (CBC), is responsible for ensuring arrangements are in place which help prevent abuse of children and vulnerable people. The Safeguarding Vulnerable Groups Act 2006 sets out the activities and work which are deemed 'Regulated Activity'. Regulated Activity is a term used to describe certain job functions carried out by an individual as defined by the Disclosure and Barring Service (DBS). These requirements are important as they determine eligibility for an Enhanced Level DBS check and a check of the DBS Barred Lists.

The correct use of Disclosure and Barring Service (DBS) checks helps ensure safe recruitment and is an important part of preventing unsuitable people from working with vulnerable groups. The council can only legally check someone's criminal record if they are applying for certain roles, where the requirement for a check has been identified. When considering the suitability of an individual for any position with access to children or vulnerable adults the authority needs to ensure that criminal record information checks are undertaken when appropriate, at the required level, and in accordance with legislative requirements. As of September 2019, CBC have 64 registered individual volunteers and 17 constituted volunteer groups. Individual volunteers will typically work at events such as the Midsummer Fiesta and the Cycling Festival and are managed at each event by a Volunteer Supervisor employed by the Council. Constituted groups such as the 'Friends of' park groups work alongside CBC Park Rangers to maintain and make improvements to parks within the Borough.

This audit was initially agreed with the HR Business Manager to review the arrangements in place to make DBS checks on volunteers where relevant to their role. At the time of audit fieldwork, there were no volunteer roles being undertaken for CBC which fall under the definition of 'Regulated Activity' and therefore no volunteers working on behalf of the Council have been subject to standard or enhanced DBS checks. The Volunteering Policy and recruiting officer guidance was therefore also reviewed as well as mitigating factors in place to safeguard children and vulnerable people in the absence of DBS checks when recruiting volunteers.

Audit Conclusion / Findings

A reasonable assurance is offered in respect of the procedures and controls in place to ensure volunteers are subject to appropriate checks and managed with safeguarding children and vulnerable groups as a priority. No significant risks were identified in the course of this audit, which is reflected in the assurance level, although some opportunities for improvement have been highlighted within the report to enhance the robustness of process and supporting information.

Residual risk (with all controls in place) has been assessed at medium by both the service area and internal audit. This is due to the potential impact of a safeguarding risk still being at a high level, even though controls in place reduce the likelihood sufficiently. Our review has shown that process and controls in place for the recruitment of volunteers at Cheltenham Borough Council (CBC) have significantly improved since the introduction of a formal Volunteering Policy which was approved by Cabinet in May 2019. A Volunteers Handbook and guidance for officers recruiting volunteers has also been published.

Seven recommendations have been made in this report; four are based on strengthening the volunteering recruitment process and controls in place already and three relate to EU General Data Protection Regulations (EU GDPR) which reflects an 'added value' element to the audit.

| Priority | Recommendation | Management Response | Due Date |
|----------|---|--|--------------------------------|
| 2 | We recommend that a copy of a constituted group's Safeguarding Policy is received and reviewed by CBC officers before the group is allowed to participate in voluntary work on behalf of the Council. | Participation and Engagement Team leaders to review Safeguarding policy process with CBC Partnership Team Leader to agree on appropriate approach. | 31 st March 2020 |
| 2 | We recommend that a link is included within the Volunteer Privacy Statement to the 'Your Data' page on the Cheltenham Borough Council website to ensure that volunteers have access to all information on their personal data required by the EU General Data Protection Regulations | To include a link within the Volunteer Privacy Statement to the 'Your Data' page on the CBC website. | 31 st December 2019 |
| 2 | We recommend that all volunteers that have signed historic version of the application form are asked to sign their consent to the current data protection arrangements and retention period. The current Volunteer Privacy Statement should also be brought to the attention of all volunteers who have not previously been made aware of it. | To strive to ensure that volunteers with historic consent forms are signed up to the 5-year data protection arrangements and retention period. | 31 st March 2020 |

2019/20 – Annual Governance Statement – Substantial Assurance

Background

Local authorities are required by the Local Audit and Accountability Act 2014 and the Accounts and Audit Regulations 2015 to prepare an Annual Governance Statement (AGS) by 31 May each year to report publicly on the extent to which they comply with their own governance and internal controls. The statement should comply with best practice and written in accordance with the CIPFA Delivering Good Governance Framework (2016).

Managers provide their assurance via an annual Manager's Assurance Statement (MAS) which is reflected in the Annual Governance Statement. Internal Audit also provide an Annual opinion in the review of effectiveness based on the audit assurances issued across the authority during the year. The draft AGS is then considered by Audit Committee in advance of the required deadline and a final version is published within the Authority's Annual Statement of Accounts.

The purpose of the audit is to review the process for producing the AGS and determine whether the completion of the AGS was based on well-founded control results and information and to ensure the AGS is produced in compliance with the correct governance framework and principles and good practice guidelines.

Audit Conclusion / Findings

The Directors and Executive Board attendees at Cheltenham Borough Council (CBC) are required to complete and return a Managers Assurance Statement (MAS) each year. The MAS is a declaration that governance measures are in place and should highlight any significant areas of concern to be included in the Annual Governance Statement (AGS). Statements are also sought from CBC affiliates such as The Cheltenham Trust and One Legal. It is noted that UBICO do not complete a statement. We can confirm 10 MAS were completed.

Seven Managers Assurance Statements were examined and were confirmed to be fully completed. However, it was noted that some of the statement templates completed varied slightly, therefore, a review of the templates used is recommended to ensure a consistent approach is taken to their completion.

The Annual Governance Statement has been measured against the Delivering Good Governance Framework document and meets the requirements and conforms to the areas of applicability and terminology. It contains detailed statements on each of the 7 core principles and sub-principles of good governance within the framework. The AGS was produced accurately and in a timely manner to meet the submission deadlines. No new significant issues were highlighted during the year, although the statement provided an update on the previous years' significant issues.

The AGS is publicly available within the Annual Statement of Accounts on the CBC website. CIPFA's Good Guidance does also suggest the statement is made available with, but separately from the Annual Statement of Accounts. CBC should consider making a separate copy of the statement for download on their website.

2018/19 – Procurement – Partial Assurance

Note

Audit fieldwork for this review was carried out between March and May 2019. All findings within this report reflect the position of the Procurement Service at that time. Early draft versions of this report were issued to the service area in June 2019 and work commenced to address some of the recommendations made. **A follow-up review of this audit is planned to be carried out in January and February 2020**, the report of which will reflect the progress made by the Procurement Service to implement agreed actions, based on evidenced information.

Background

This audit review focuses on the procurement processes undertaken on behalf of West Oxfordshire District Council (WODC), Cotswold District Council (CDC), Cheltenham Borough Council (CBC) and Forest of Dean District Council (FODDC). Procurement Officers support Officers located across all client sites.

Procurement activity must be undertaken in accordance with Contract Rules, and;

- Procurement and contract management strategy (2015)
- National Procurement Strategy (2018)
- The Public Contracts Regulations (2015)
- Local Government Transparency Code (2015)

Testing was undertaken using the overarching Contract Register (February 2019) and we were provided with requisitioning and approving data from the financial management system (March 2019). Due to the format in which contract values have been recorded on the Contract Register, we have been unable to calculate the total value of all contracts across each organisation. A total of 153 contracts were included on the register and of these, 67 had a recorded end date which had passed at the time of audit work (March 2019) and 4 had no end date recorded.

Audit Conclusion / Findings

The financial management system (ABW) and Procurement portal (In-Tend) are not linked, so a full audit trail of procurement activity is not recorded within one central system. When Procurement Business Partners are requested to

enter approved contracts onto In-Tend a record is created, all relevant documentation for approved contracts is recorded within the portal. All approved financial transactions are recorded within ABW.

Service areas are responsible for reviewing their financial management system authorisation limits, and we were advised all changes to permissions are logged through the helpdesk and must be authorised by the appropriate line manager or a finance officer. User ID's and authorisation limits were examined for a sample of Officers to assess whether approval limits are as expected for their job role and organisation. At the time of testing, a significant restructuring of Publica was underway; we would therefore suggest requisitioning and authorisation permissions are reviewed in line with the new Publica organisational structure.

At the time of audit work, Procurement were not informed of all approved contracts with a value of £5,000 and over as per process, so there was a risk the Contract Register was not a complete record. Since testing, we have been advised contract reports are now generated from the procurement portal and financial management system to provide contract data which is amalgamated into an overarching Contract Register. Testing was undertaken to assess if the details recorded on the register are complete and accurate; none of the contracts in our sample had a copy of the approved contract saved on the procurement portal as per process, so we were unable to assess if the Contract Register was an accurate record. Going forward, once approved, a copy of the contract must be saved against the contract entry on the portal; keeping this record will also help to support that separation of duties has been maintained.

At the time of audit work, different versions of the Contract Register were published on the Council websites; to ensure transparency and information is current and accurate, the same version of the Contract Register must be published on all Council websites quarterly.

At the time of audit work, the Contract Register had not been reviewed on a quarterly basis as per process due to limited resource. We were advised a piece of work to update the Contract Register for all clients was being actioned by Procurement, and a Purchase Order for development with Contract Wizards setups and training had been actioned to mitigate against this; we agree this will be beneficial to all clients.

Testing was undertaken to assess whether waivers are applied in accordance with Contract Rules; not all the waivers selected were completed in line with guidance, and a copy of only 1 waiver was saved against the contract entry on the

procurement portal. For the waivers selected, an entry on the Contract Register could not be found for all contracts, and none of the contracts entered had a copy of the approved contract saved on the procurement portal. Procurement must be informed of all waivers so this detail can be recorded to ensure transparency. Although each Council's solicitor must keep a copy of the agreed waiver, a record should also be maintained to support the decision for applying the waiver; we were advised Procurement will be implementing a Waiver Register later in 2019.

Our review has found procurement processes are not all undertaken in accordance with Contract Rules and policy. From our discussions and the evidence provided, controls and policy guidance are in place, but testing supports procurement activity is not always undertaken in accordance with these agreed processes. Since the time of audit work, we were advised that processes relating to the population of the Contract Register have been reviewed by the Publica Procurement Business Partner, the Procurement Portal is now accessible from all Council websites, and further work has been planned to implement a Procurement Waiver Register. We were also advised that the Contracts Module on In-Tend has a planned roll out date of July; this will help to rectify the findings above which relate to contract documentation not being recorded centrally. The Procurement and Contract Management Strategy will be reviewed with the Counter Fraud Unit in 2019, and at the time of audit work, evidence was seen to support training on procurement process and Contract Rules was due to be delivered across all clients, and improvements were due to be made to the procurement portal. This is essential to improve Officer knowledge, embed procurement processes and controls across all clients to ensure they are followed correctly and in accordance with regulations and Council policy, and improve communication channels between all Service Areas and Procurement.

Publica Management Response to the Audit Findings

In response to the Procurement and the Procurement and Contract Management audit reports issued, we plan to carry out a fundamental review of the Procurement Service. This review will include an evaluation of how the Procurement Service will integrate or work alongside the new Commissioning and Contract Management teams introduced as part of the recent service review.

| Priority | Recommendation | Management Response | Due Date |
|----------|--|---|--------------------------------------|
| 2 | A copy of the approved contract must be held on In-Tend for all contracts over £5,000, as well as the quotes used during the tendering process, to demonstrate best value and ensure there is a complete central record. | Agreed, subject to a review of the contract value requirements. | 31 st December 2019 |
| 2 | Budget Holders should regularly undertake monitoring of | Agreed | 31 st |

| | | | |
|---|--|--|--------------------------------|
| | expected contract spend to actual contract spend as part of contract monitoring, to ensure contracts are managed in accordance with strategy, and inform Procurement of any changes to contract values to ensure the values recorded on the Contract Register are correct. | | December 2019 |
| 2 | To ensure there is an audit trail to support all contract payments, the introduction of "No PO, no payment" policy should be considered to assist with the efficient monitoring of contract spend. | This will be considered | 31 st December 2019 |
| 2 | To ensure there is a central record, when a waiver has been applied, this must be logged on the Waiver register once it has been implemented, for transparency purposes. | Agreed | 31 st December 2019 |
| 2 | All Officers should be informed during Procurement Process training of the following to ensure when applicable; • Procurement are consulted on all contracts over £5,000 so all approved contracts are entered onto the Contract Register, and waiver details can be accurately recorded when appropriate | Agreed | 31 st December 2019 |
| 2 | To ensure all transactions are raised and approved appropriately and in line with the current organisational structure, all requisitioning and approval permissions should be reviewed in BWO. | Following the recent organisation changes, the approvals permissions will be reviewed to ensure they are aligned with new roles and implemented accordingly on the ABW system. | 31 st December 2019 |
| 2 | CBC must liaise with One Legal to ensure all waivers approved by Cabinet are also retained by the Council's Solicitor, in accordance with the Council's Contract Rules. | Waivers granted by Cabinet would form part of the committee report which are held by democratic services. In order to prevent multiple copies being held, the contract rules will be amended to reflect this action. | 31 st December 2019 |

High Priority Recommendation Follow-Up

APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update January 2020 |
|--|----------|--|---|----------|---|
| 2018/19 Business Continuity Management | 2 | Consideration could be given to aligning the BCP with the international standard ISO22301, as this provides a framework to plan, establish, implement, operate, monitor, review, maintain and continually improve a business continuity management system. | Consideration will be given to aligning the BCP with the international standard ISO22301 following the review of the Business Continuity Planning process which will be undertaken by the Civil Protection Team after April 2019. | 30/06/19 | Follow up in progress. |
| 2018/19 Business Continuity Management | 2 | Consideration should be given to the clarity of the existing template and its ability to guide an officer in difficult and stressful times, and adopting an existing template, to better meet the authority's responsibilities. | An independent review of the CBC BCPs has been agreed with the Civil Protection Team this will commence after April 2019 when resources become available. The Corporate BCP will be identified as the first plan to be reviewed. | 30/06/19 | Follow up in progress. |
| 2018/19 Business Continuity Management | 2 | Consideration could be given to the utilising the out of hours automated phone system, already in place, as an emergency information line for providing information to staff and / or the public if other methods of communication are down. | Consideration will be given to utilising the out of hours automated phone system already in place as an emergency information line after the review of the Business Continuity Plans. | 30/06/19 | Follow up in progress. |
| 2018/19 Accounts Receivable | 2 | A review of all active subscriptions should be carried out, on behalf of each client, to identify any other duplicate subscriptions and these should all be corrected. Priority | Agreed. This will be carried out. Additional training will also be provided to AR officers to prevent this occurring again in the future. | 31/03/19 | Will be followed up during the annual audit of Accounts Receivable. |

High Priority Recommendation Follow-Up

APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update January 2020 |
|--|----------|---|--|----------|--|
| 2018/19 Members' and Officers' Gifts, Hospitality and Declarations of Interest | 2 | We recommend that consideration is given to work between CBC and the Counter Fraud Unit (CFU) to refresh the approach to the declarations process as part of their planned work discuss the introduction of a risk-based approach to conflict of interest forms in 2019/20. Priority | The CFU manager agrees to review this with the support of SWAP and Governance Group as part of the 2019/2020 work plan. The Programme Manager agrees to work with the CFU to review their risk-based approach and see if this is appropriate for implementation at CBC. | 31/03/20 | Work ongoing. |
| 2018/19 Members' and Officers' Gifts, Hospitality and Declarations of Interest | 2 | We recommend that actions are taken to increase officer awareness on the responsibility to declare interests, gifts and hospitality. This may include (but not be limited to): - Regular reminders posted on the staff intranet - Sending out email reminders - Periodic training | The Programme Manager agrees to increase officer awareness through reminders on a quarterly basis and ensure periodic training is undertaken. | 30/04/19 | We were advised that this recommendation will be actioned via a new learning & development system that has been purchased. Agreed to extend implementation date to 30/06/20. |

High Priority Recommendation Follow-Up

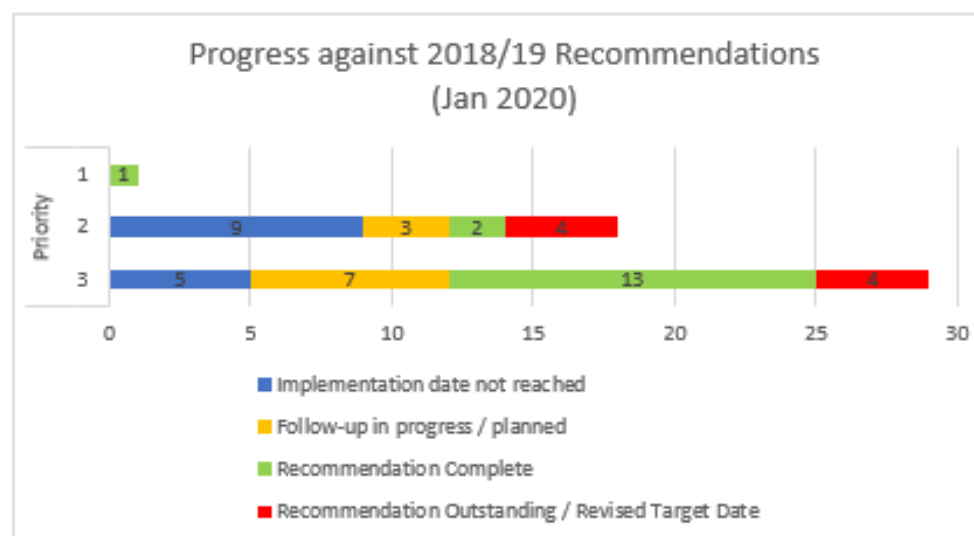
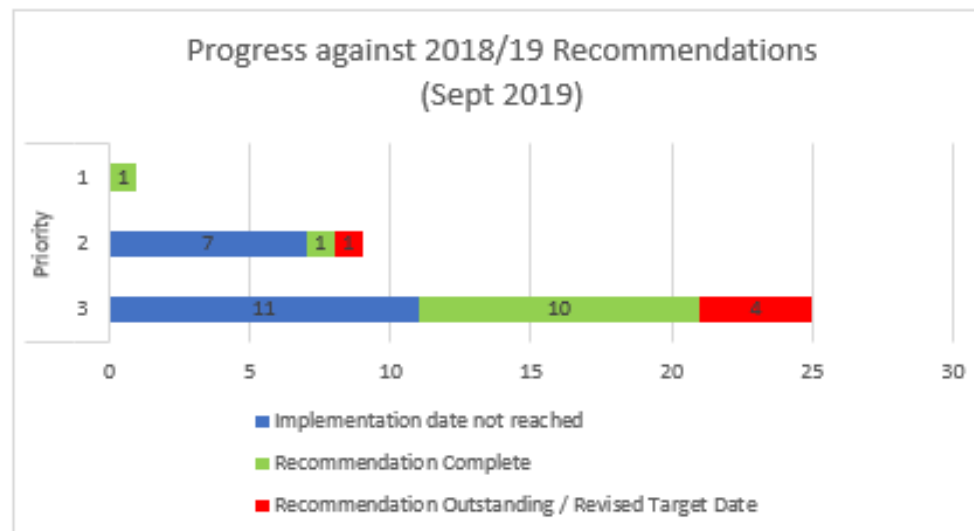
APPENDIX D

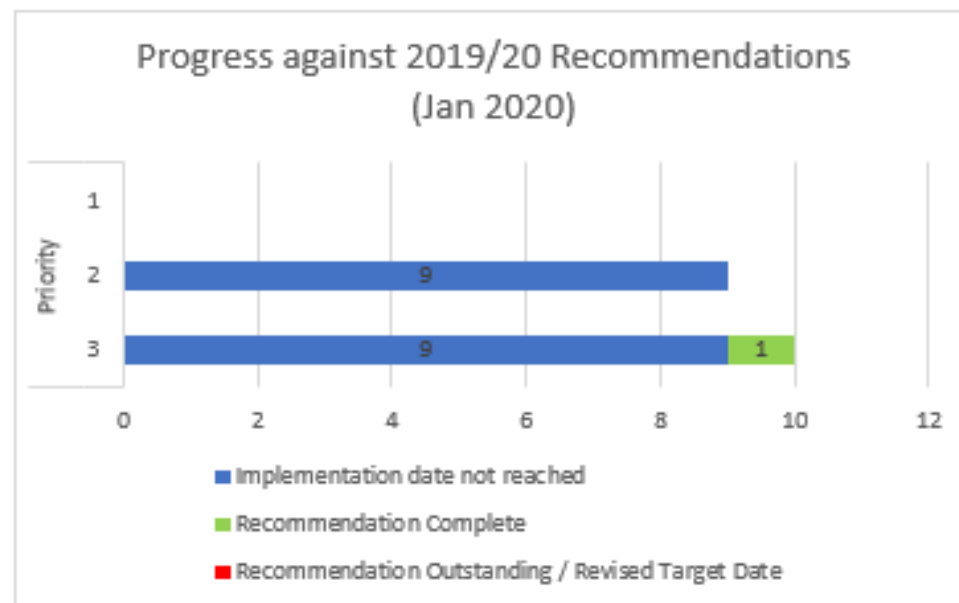
| Audit Name | Priority | Recommendation | Management Response | Due Date | Update January 2020 |
|-----------------------|----------|---|--|----------|---------------------|
| 2018/19 Systems Admin | 2 | <p>We recommend a principal Identity and Access Management process detailing requirements for 'Joiners, Movers and Leavers' is developed and documented and that complies with the requirements set out in the Information Security and Access Control Policy. The overarching process should apply to and embrace all systems that may not be included within the standard ICT team scope and should be available for all employees to view and follow.</p> <p>System administrators should then document or update local processes and procedures that should be in alignment with the overarching policy and process requirements. and documented on a quarterly basis as per the requirements of the Risk Management Policy</p> | Our team ICT Administrators are now updating and documenting our Access Management system process for joiners, Movers and Leavers. A change control process will be introduced that will document significant changes to the ICT infrastructure which will also align to our ICT User Policies and guidance. | 31/03/20 | |

High Priority Recommendation Follow-Up

APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update January 2020 |
|-----------------------|----------|---|--|----------|-----------------------|
| 2018/19 Systems Admin | 2 | We recommend that officers with systems administration responsibilities are requested to review the Security Policy and its requirements, perform a gap analysis on their current system settings and processes and devise a plan to implement those changes to ensure continued compliance with the Policy. Should it not be possible to make changes for any reason, they should be risk assessed and documented on the ICT risk register or policy exception register. | We agree with the password setting findings and risks with on systems Business World and Civica applications. However, at present these risks are mitigated by the Active Directory (AD) password settings. Both Business world and Civica systems users only access these systems via the AD. We also comply with the HMG National Cyber Security Centre (NCSC) password guidance on our network. However, we will seek to review all passwords policy setting on both applications. Our ICT Risk register will be updated to reflect these security risks and mitigations. | 31/12/19 | Follow-up in progress |





Audit, Compliance and Governance Committee – 22 January 2020

Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy

Investigatory Powers Act 2016 Acquisition of Communications Data Policy

| | |
|---------------------------------|--|
| Accountable Member | Cabinet Member Corporate Services, Councillor Alex Hegenbarth |
| Accountable Officer | Acting Chief Executive Tim Atkins, Managing Director Place and Growth Tim.Atkins@cheltenham.gov.uk |
| Ward(s) affected | All indirectly |
| Key/Significant Decision | No |
| Executive summary | <p>To present Cabinet with:</p> <ul style="list-style-type: none"> i) A revised Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy for approval and adoption. ii) A new Investigatory Powers Act 2016 Acquisition of Communications Data Policy for approval and adoption. <p>The Local Authority is required to have effective Policies to enable officers to gather intelligence and conduct surveillance in line with the law.</p> <p>The Policies set out the legislative framework and principles the Local Authority will abide by to mitigate the risk of legal challenge in Court.</p> <p>The Policy demonstrates the Local Authority's consideration of necessity, proportionality and public interest when deciding on surveillance activity and requests for communication data. It also demonstrates openness and transparency for its customers.</p> <p>The report also provides an update in relation the Local Authority's existing authorisation arrangements.</p> |
| Recommendations | <p>That the Audit, Compliance and Governance Committee:</p> <ul style="list-style-type: none"> a) Considers the Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy to comment thereon to Cabinet, to aid its deliberations and decision making. b) Considers the Investigatory Powers Act 2016 Acquisition of Communications Data Policy to comment thereon to Cabinet, to aid its deliberations and decision making. |

| | |
|--|--|
| Financial implications | <p>The adoption and approval of these Policies will support the Local Authority's objectives in reducing crime and financial loss to the Local Authority.</p> <p>Contact Officer: Paul Jones, Executive Director Finance and Assets Paul.Jones@cheltenham.gov.uk</p> |
| Legal implications | <p>The Local Authority is required to ensure that it complies with the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and any other relevant/statutory legislation regarding investigations. It should also consider government guidance in this area.</p> <p>The Local Authority has a statutory obligation for enforcing a wide range of legislation, where it is necessary and proportionate to do so. Human rights implications are a consideration of this type of activity and this is included within the Policy.</p> <p>Any requests for directed/covert surveillance or the acquisition of communications data to be undertaken should be necessary and proportionate, and authorised by the appropriate Officer. Both Policies provide information and advice to those seeking authorisation and those officers granting authorisation. Both policies confirm the process to be used and matters to be considered.</p> <p>Contact officer: Iona Moseley, One Legal. iona.moseley@teWKesbury.gov.uk</p> |
| HR implications (including learning and organisational development) | <p>There will be a requirement to cascade the new policies to all relevant employees and ensure any training is undertaken.</p> <p>Contact officer: Julie McCarthy, HR Operations Manager Julie.McCarthy@publicagroup.uk 01242 264355</p> |
| Key risks | <p>The Policies demonstrate the Local Authority's consideration of necessity, proportionality and public interest when deciding on surveillance activity or the decision to obtain personal communication data.</p> <p>The Policies set out the legislative framework and principles the Local Authority will abide by in investigations undertaken to mitigate the risk of legal challenge in Court.</p> |
| Corporate and community plan Implications | <p>Effective enforcement plays an important role in enabling the Local Authority to achieve its priorities and community outcomes.</p> |
| Environmental and climate change implications | <p>N/A</p> |
| Property/Asset Implications | <p>There are no property implications associated with this report.</p> <p>Contact officer: Dominic Stead, Head of Property Services dominic.stead@cheltenham.gov.uk</p> |

1. Background

- 1.1. The Local Authority's Policies are based on the legislative requirements of the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and the Codes of Practice relating to directed surveillance, the use of covert human intelligence sources and the acquisition of communications data. Attached at [Appendix 2](#) and at [Appendix 3](#) are revised Policies.
- 1.2. The Investigatory Powers Act 2016 now governs communication data requests. The legislation widened the scope of information the Local Authority may obtain for investigations, introduced the necessity for a serious crime threshold and removed the requirement for judicial approval.
- 1.3. All applications for communications data are made online via the National Anti-Fraud Network (NAFN) which acts as the single point of contact for Local Authorities. NAFN send requests to the Office for Communication Data Authorisations (OCDA) which ratifies all applications from public authorities for approval and if granted, NAFN will then obtain the requested data for the applicant.
- 1.4. There is a requirement for the Local Authority to nominate a Designated Senior Officer who will confirm to NAFN that the Local Authority is aware of any request and approve its submission. This role is undertaken by the Counter Fraud Manager and the Deputy Counter Fraud Manager.
- 1.5. Surveillance and the use of a Covert Human Intelligence Source (CHIS) is still governed by the Regulation of Investigatory Powers Act 2000 and any 'RIPA' applications are subject to the same application processes as outlined in the previous Policy – the offence must meet the serious crime threshold and the Local Authority must obtain judicial approval.
- 1.6. As outlined in 1.5 above, the Local Authority must have a Senior Responsible Officer and Authorising Officers to approve the application before the Court is approached. The arrangements relating to Officers involved in the authorisation process have been updated to reflect the changes in staffing.
- 1.7. The Senior Responsible Officer is the Acting Chief Executive, Tim Atkins and the Authorising Officers are the Executive Director People and Change, Darren Knight and the Director of Environment, Mike Redman.
- 1.8. The refreshed Policy introduces a mandatory requirement for staff to complete a Non-RIPA Application Form where surveillance is being undertaken but the offence does not meet the serious crime criteria.
- 1.9. As reported in April 2019, there were no RIPA applications made by the Local Authority during 2018/2019. There were four Non-RIPA applications made during 2018. Three related to overt activity and one related to an internal investigation.
- 1.10. The application of these Policies, to govern surveillance and the obtaining of personal communications data, ensures that there is less risk that an individual's human rights will be breached. Furthermore it protects the Local Authority from allegations of the same.

2. Consultation

- 2.1. The draft Policy was subject to consultation with Enforcement Officers, Governance Group, Executive Leadership Team and One Legal.

| | |
|----------------------|---|
| Report author | Emma Cathcart, Counter Fraud Manager Emma.Cathcart@cotswold.gov.uk 01285 623356 |
| Appendices | <ol style="list-style-type: none">1. Risk assessment2. Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy3. Investigatory Powers Act 2016 Acquisition of Communications Data Policy |

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 | Likelihood 1-6 | Score | Control | Action | Deadline | Responsible officer | Transferred to risk register |
| 1 | If the Local Authority fails to put in place adequate policy and process covering the use of RIPA / IPA powers then it risks damage to its reputation and financial loss | Chief Executive | January 2020 | 4 | 2 | 8 | | Put in place effective management and guidance. Promote the guidance with managers and enforcement officers | Ongoing | Chief Executive | |
| 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

| | |
|-----------------------------|--|
| Version Control: | |
| Document Name: | Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy |
| Version: | 2 |
| Responsible Officer: | Emma Cathcart, Counter Fraud Unit |
| Approved by: | Cabinet |
| Date First Approved: | TBC |
| Next Review Date | |
| Retention Period: | N/A |

Revision History

| Revision date | Version | Description |
|---------------|---------|--|
| April 2019 | 2 | Change in legislation / introduction of IPA 2016 |
| | | |

Consultees

| Internal | External |
|----------------------|----------|
| Audit Committee | |
| Legal Department | |
| Corporate Management | |

Distribution

| Name | |
|----------------------|--|
| Enforcement Officers | |
| | |

CONTENTS

| | |
|--|----|
| 1. INTRODUCTION | 4 |
| 2. SCOPE OF POLICY | 4 |
| 3. BACKGROUND | 5 |
| 4. SURVEILLANCE WITHOUT RIPA..... | 5 |
| 5. INDEPENDENT OVERSIGHT | 6 |
| 6. LEGAL ADVICE | 6 |
| 7. REVIEW OF POLICY AND PROCEDURE..... | 6 |
| 8. RIPA ROLES AND RESPONSIBILITIES..... | 7 |
| 8.1 THE SENIOR RESPONSIBLE OFFICER | 7 |
| 8.3 THE RIPA COORDINATOR..... | 7 |
| 8.6 INVESTIGATING OFFICER/APPLICANT | 8 |
| 8.9 AUTHORISING OFFICERS | 8 |
| 9. SURVEILLANCE TYPES AND CRITERIA | 9 |
| 9.4 OVERT SURVEILLANCE | 9 |
| 9.6 COVERT SURVEILLANCE | 9 |
| 9.9 INTRUSIVE SURVEILLANCE..... | 10 |
| 9.14 DIRECTED SURVEILLANCE | 10 |
| 10. PRIVATE INFORMATION | 11 |
| 11. CONFIDENTIAL OR PRIVILEGED MATERIAL | 11 |
| 12. INTERNET AND SOCIAL MEDIA INVESTIGATIONS | 12 |
| 13. CCTV | 12 |
| 14. AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)..... | 12 |
| 15. JOINT AGENCY SURVEILLANCE | 12 |
| 16. USE OF THIRD PARTY AGENTS..... | 13 |
| 17. EQUIPMENT | 13 |
| 18. COVERT HUMAN INTELLIGENCE SOURCES (CHIS)..... | 13 |
| 18.9 DEFINITION OF CHIS | 14 |
| 18.19 VULNERABLE CHIS | 15 |
| 18.24 USE OF EQUIPMENT BY A CHIS | 16 |
| 18.27 CHIS MANAGEMENT | 16 |
| 18.30 CHIS RECORD KEEPING..... | 16 |
| 19. NECESSITY | 17 |
| 20. PROPORTIONALITY | 17 |
| 21. COLLATERAL INTRUSION..... | 18 |
| 22. THE APPLICATION AND AUTHORISATION PROCESS..... | 18 |
| 22.2 DURATION OF AUTHORISATIONS..... | 18 |

| | | |
|-------|--|----|
| 22.5 | APPLICATIONS/AUTHORISATION..... | 19 |
| 22.15 | ARRANGING THE COURT HEARING | 20 |
| 22.18 | ATTENDING THE HEARING | 20 |
| 22.23 | DECISION OF THE JP | 20 |
| 22.32 | POST COURT PROCEDURE | 21 |
| 22.35 | MANAGEMENT OF THE ACTIVITY | 21 |
| 22.37 | REVIEWS..... | 21 |
| 22.44 | RENEWAL | 22 |
| 22.52 | CANCELLATION..... | 23 |
| 23. | SURVEILLANCE OUTSIDE OF RIPA | 23 |
| 24. | SAFEGUARDING AND THE USE OF SURVEILLANCE MATERIAL..... | 24 |
| 24.2 | AUTHORISED PURPOSE | 24 |
| 24.1 | USE OF MATERIAL AS EVIDENCE | 25 |
| 24.6 | HANDLING AND RETENTION OF MATERIAL..... | 25 |
| 24.13 | DISSEMINATION OF INFORMATION | 26 |
| 24.17 | STORAGE..... | 26 |
| 24.19 | COPYING..... | 26 |
| 24.22 | DESTRUCTION | 27 |
| 25. | ERRORS..... | 27 |
| 25.2 | RELEVANT ERROR | 27 |
| 25.6 | SERIOUS ERRORS | 27 |
| 26. | COMPLAINTS | 28 |

1. INTRODUCTION

- 1.1 The performance of certain investigatory functions by Local Authorities may require the surveillance of individuals or the use of undercover Officers and informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates these types of activities and the Act and this Policy must be followed at all times.
- 1.2 Neither RIPA nor this Policy covers the use of any overt surveillance, or general observation that forms part of the normal day to day duties of Officers, or circumstances where members of the public volunteer information to the Council. The majority of the Council's enforcement functions are carried out in an overt manner.
- 1.3 RIPA was introduced to ensure that public authorities' actions are consistent with the Human Rights Act 1998 (HRA). It balances safeguarding the rights of the individual against the needs of society as a whole to be protected from crime and other public safety risks. This reflects the requirements of Article 8 (right to privacy) under the HRA. RIPA provides a statutory mechanism for authorising covert surveillance and the use of a covert human intelligence source (CHIS).
- 1.4 RIPA also introduced a legal gateway for public authorities to apply for telecommunications and postal data. However, these have been amended by the Investigatory Powers Act 2016 (IPA), and for guidance in relation to the obtaining of Communications Data please see the IPA Acquisition of Communications Data Policy.

2. SCOPE OF POLICY

- 2.1 The purpose of this document is to ensure that the Council complies with RIPA.
- 2.2 This document provides guidance on the regulation of any Directed Covert Surveillance that is carried out by the Council. This includes the use of undercover Officers and informants, known as Covert Human Intelligence Sources (CHIS).
- 2.3 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.
- 2.4 All directed surveillance must be authorised and conducted in accordance with RIPA. Therefore, all Officers involved in the process must have regard to this document and the statutory Codes of Practice issued under section 71 RIPA. The Codes of Practice are available from:
<https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice>
- 2.5 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 and the RIPA Codes of Practice.
- 2.6 Any queries concerning the content of the document should be addressed to the RIPA Coordinator, Counter Fraud Unit.

3. BACKGROUND

- 3.1 RIPA provides a legal framework for the control and regulation of covert surveillance techniques which public authorities undertake as part of their duties. As was highlighted in the introduction to this Policy, the need for such control arose as a result of the HRA. 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.
- 3.2 The right under Article 8 is a qualified right and public authorities can interfere with this right for the reasons given in 2.3 above. RIPA provides the legal framework for lawful interference.
- 3.3 However, under RIPA, Local Authorities can only authorise directed covert surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is:
- An offence that is capable of attracting a maximum prison sentence of 6 months or more punishable whether on summary conviction or indictment meets the serious crime threshold or,
 - Relates to the underage sale of alcohol or tobacco.
- 3.4 Furthermore, the Council's authorisation can only be given effect once an Order approving the authorisation has been granted by a Justice of the Peace (JP).
- 3.5 The serious crime criteria do not apply to CHIS authorisations.
- 3.6 RIPA ensures that any surveillance undertaken following a correct authorisation and approval from a JP is lawful and therefore protects the Council from legal challenge. It allows the information obtained to be used as evidence in the investigation. It can also be used if required in other investigations.

4. SURVEILLANCE WITHOUT RIPA

- 4.1 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.
- 4.2 Lawful surveillance is exempted from civil liability.
- 4.3 Although not obtaining authorisation does not make the surveillance unlawful per se, it does have some consequences:-
- Evidence that is gathered may be inadmissible in court;
 - 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;
 - If a challenge under Article 8 is successful, the Council could face a claim for financial compensation;

- The Government has also introduced a system of tribunal to deal with complaints. Any person who believes that their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPTC) (See Complaints section within the Code of Practice)

5. INDEPENDENT OVERSIGHT

- 5.1 From 1 September 2017 oversight of RIPA is provided by the Investigatory Powers Commissioner's Office (IPCO). They are the independent inspection office whose remit includes providing comprehensive oversight of the use of the powers to which the RIPA Codes of Practice apply, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes.
- 5.2 Anyone, including anyone working for the Council, who has concerns about the way that investigatory powers are being used, may report their concerns to the IPCO
- 5.3 IPCO has unfettered access to all locations, documentation and information systems as is necessary to carry out its full functions and duties and it will periodically inspect the records and procedures of the Council to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.
- 5.4 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information required for the purpose of enabling them to carry out their functions.
- 5.5 It is important that the Council can show it complies with this Policy and with the provisions of RIPA.

6. LEGAL ADVICE

- 6.1 The Council's legal representatives will provide legal advice to staff making, renewing or cancelling authorisations. Requests and responses for legal advice will be in writing and copied to the RIPA Coordinator, Counter Fraud Unit to keep on file.

7. REVIEW OF POLICY AND PROCEDURE

- 7.1 The Audit Committee will receive annual reports regarding the use of RIPA. Those reports will contain information on:
- Where and when the powers have been used;
 - The objective;
 - The authorisation process;
 - The job title of the Senior Responsible Officer (SRO), Authorising Officers (AO) and RIPA Coordinator;
 - The outcomes including any legal court case;
 - Any costs.

8. RIPA ROLES AND RESPONSIBILITIES

8.1 THE SENIOR RESPONSIBLE OFFICER

8.2 The SRO has responsibility for the following:

- The integrity of the process in place within the Council to authorise Directed and Intrusive Surveillance;
- Compliance with the relevant sections of RIPA and the Codes of Practice;
- Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the IPCO and the inspectors who support the IPC when they conduct their inspections;
- Where necessary, overseeing the implementation of any recommended post-inspection action plans and;
- Ensuring that all AO are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the IPC.

8.3 THE RIPA COORDINATOR

8.4 The RIPA Coordinator is responsible for storing all the original authorisations, reviews, renewals and cancellation forms and the signed approval or refusal documentation from the JP. This will include any authorisations that have not been authorised by the AO or refused by a JP.

8.5 The RIPA Coordinator will:

- Keep the copies of the forms for a period of at least 3 years;
- Keep the Central Register (a requirement of the Codes of Practice) of all of the authorisations, renewals and cancellations; and issue a unique reference number. This record should contain the information outlined within the Covert Surveillance and Property Interference revised Code of Practice;
- Keep a database for identifying and monitoring expiry dates and renewal dates;
- Along with Officers (AO and Investigating Officers (IO)), ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Council's Information Management Policies, Departmental Retention Schedules and Data Protection Legislation /Regulations;
- Provide administrative support and guidance on the processes involved;
- Not provide legal guidance or advice;
- Monitor the authorisations, renewals and cancellations with a view to ensuring consistency throughout the Council;
- Monitor each department's compliance and act on any cases of non-compliance;
- Provide training and further guidance and awareness of RIPA and the provisions of this Policy; and review the contents of this Policy.

8.6 INVESTIGATING OFFICER/APPLICANT

8.7 The applicant is normally an IO who completes the application section of the RIPA form. IOs should think about the need to undertake directed surveillance or the use of a CHIS before they seek authorisation. IOs must consider whether they can obtain the information by using techniques other than covert surveillance. Advice can be given by the RIPA Coordinator.

8.8 The applicant or IO must carry out a feasibility study and this should be seen by the AO. The IO seeking authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any significant delay between the feasibility study and the completion of the application form in order to ensure that the details within the application are accurate. The form should then be submitted to the AO for authorisation.

8.9 AUTHORISING OFFICERS

8.10 The role of the AO is to authorise, review, renew and cancel directed surveillance.

8.11 AOs should not be responsible for authorising investigations or operations in which they are directly involved. Where an AO authorises such an investigation or operation the Central Record of Authorisations should highlight this, and it should be brought to the attention of the ICO or Inspector during their next inspection.

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

8.13 A designated AO must qualify both by rank and by competence. Officers who wish to be designated must have been trained to an appropriate level in order to have an understanding of RIPA and the requirements that must be satisfied before an authorisation can be granted.

8.14 Authorisations must be given in writing by the AO by completing the relevant section on the authorisation form. Before giving authorisation for directed surveillance, an AO 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.

8.15 The lawful criteria for CHIS are prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of 6 months imprisonment but consideration must be given to the risk of collateral intrusion (the risk of obtaining private information about persons who are not the subject of investigation), the possibility of collecting confidential personal information and that the result cannot reasonably be achieved by any other means.

8.16 When completing an authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

8.17 The application should explain why the activity is both necessary and proportionate, having regard to the collateral intrusion. It should also explain exactly what is being authorised, against whom, in what circumstances, where

and so on, and that the level of the surveillance is appropriate to achieve the objectives. It is important that this is very clear as the surveillance operatives will only be able to carry out activity that has been authorised. This will assist with avoiding errors.

- 8.18 If any equipment such as covert cameras are to be used, the AO should know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. It is important that they consider all the facts to justify their decision and that it is not merely a rubber-stamping exercise.
- 8.19 The AO may be required to attend court to explain what has been authorised and why. Alternatively, they may have to justify their actions at a tribunal. AOs are also responsible for carrying out regular reviews of applications, for authorising renewals and cancelling any authorisation (see relevant sections below).
- 8.20 AOs must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and the current Procedures and Guidance issued by the Commissioner. This document also details the latest operational guidance to be followed. It is recommended that AOs hold their own copy of this document.
- 8.21 AOs, through the Council's Data Controller, must ensure compliance with the appropriate data protection requirements under data protection legislation and regulation and any relevant internal protocols of the Council relating to the handling and storage of material.

9. SURVEILLANCE TYPES AND CRITERIA

9.1 Surveillance is:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- Recording anything monitored, observed or listened to in the course of surveillance, with or without the assistance of a device.

9.2 By its very nature, surveillance may involve invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are within at the time. For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers out into public areas.

9.3 There are different types of surveillance which, depending on their nature, are either allowable or not allowable and that require different degrees of authorisation and monitoring under RIPA.

9.4 OVERT SURVEILLANCE

9.5 Overt surveillance is where the subject of surveillance is aware that it is taking place. This could be by way of signage, such as in the use of CCTV, or because the subject of the surveillance has been informed of the activity. Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. However, it still must take account of privacy under the HRA.

9.6 COVERT SURVEILLANCE

- 9.7 Covert Surveillance is defined as “surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place” and is covered by RIPA. Covert surveillance is categorised as either intrusive or directed.
- 9.8 There are three categories of covert surveillance regulated by RIPA:
- 1) **Directed Surveillance;**
 - 2) **Covert Human Intelligence Sources (CHIS);** and
 - 3) **Intrusive surveillance** (the Council is not permitted to carry out intrusive surveillance).
- 9.9 INTRUSIVE SURVEILLANCE
- 9.10 The Council has no authority in law to carry out Intrusive Surveillance. Intrusive surveillance is defined in section 26(3) of RIPA as covert surveillance that:
- Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
 - Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.
- 9.11 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive 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. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.
- 9.12 A risk assessment of the capability of equipment being used for surveillance of residential premises and private vehicles should be carried out to ensure that it does not fall into intrusive surveillance.
- 9.13 If you are considering conducting surveillance that may fall within the scope of intrusive surveillance you must contact the RIPA Coordinator for clarification or seek legal advice from the legal department before you undertake any surveillance.
- 9.14 DIRECTED SURVEILLANCE
- 9.15 Surveillance is directed surveillance within RIPA if the following are applicable:
- It is covert, but not intrusive surveillance;
 - It is conducted for the purposes of a specific investigation or operation;
 - It is likely to result in the obtaining of private information (see private information below) about a person (whether or not one specifically identified for the purposes of the investigation or operation);
 - It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.
 - The offence under investigation attracts a maximum custodial sentence of six months, or it is an investigation into 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.

10. PRIVATE INFORMATION

- 10.1 The Code of Practice provides guidance on the definition of private information and states it includes any information relating to a person's private or family life. As a result, private information is capable of comprising any aspect of a person's relationship with others including family and professional or business relationships.
- 10.2 Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.
- 10.3 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public, and where a record is being made by the Council of that person's activities for future consideration or analysis.
- 10.4 Surveillance of publicly accessible areas of the internet should be treated in a similar way particularly when accessing information on social media websites. (See the Internet and Social Media Research and Investigations Policy for further guidance)
- 10.5 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish a pattern of behaviour. Consideration must be given if one or more pieces of information (whether or not available in the public domain) are covertly and / or overtly obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.
- 10.6 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate

11. CONFIDENTIAL OR PRIVILEGED MATERIAL

- 11.1 Particular consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged; confidential journalistic material or where material identifies a journalist's source; or material containing confidential personal information or communications between a Member of Parliament and another person on constituency business. Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material must be authorised by the SRO. Advice should be sought from the RIPA Coordinator and the Legal Department if there is a likelihood of this occurring.

12. INTERNET AND SOCIAL MEDIA INVESTIGATIONS

- 12.1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.
- 12.2 The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks. The activity may also require RIPA authorisations for Directed Surveillance or CHIS. Where this is the case, the application process and the contents of this policy are to be followed.
- 12.3 There is a detailed Internet and Social Media Research and Investigations Policy that covers online open source research which should be read and followed in conjunction with this policy.

13. CCTV

- 13.1 The use of the CCTV systems operated by the Council does not normally fall under the RIPA regulations. However, it does fall under the data protection legislation and regulations, the Surveillance Camera Code 2013 and the Council's CCTV Policy. However, should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under directed surveillance and therefore require an authorisation under RIPA. The Council's CCTV Policy and Procedures should be referred to.
- 13.2 If an IO envisages using any other CCTV system they should contact the RIPA Coordinator concerning any clarification on the administrative process or seek legal advice before they undertake any surveillance.

14. AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

- 14.1 Automated Number Plate Recognition (ANPR) does not engage RIPA if it is used for the purpose it is registered for, such as traffic flow management or safety and enforcement within car parks. However, it is capable of being a surveillance device if used in a pre-planned way to carry out surveillance by monitoring a particular vehicle or by plotting its locations, e.g. in connection with illegally disposing of waste.
- 14.2 Should it be necessary to use the Police ANPR systems to monitor vehicles, the same RIPA principles apply regarding when a directed surveillance authorisation should be sought.

15. JOINT AGENCY SURVEILLANCE

- 15.1 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.

- 15.2 Council staff involved with joint agency surveillance must ensure that all parties taking part are authorised on the form to carry out the activity. When Council Officers 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 Coordinator at the Council to assist with oversight and monitoring.

16. USE OF THIRD PARTY AGENTS

- 16.1 In some circumstances it may be appropriate or necessary for the Council to work with third parties who are not themselves a public Authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of the Council, then they are acting as our agent and any activities that the third party conducts which meet the RIPA definitions of directed surveillance should be authorised. The agent will be subject to RIPA in the same way as any employee of the Council would be. The AO 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 the Legal Department.
- 16.2 If the above circumstances apply and it is intended to instruct an agent to carry out the covert activity, the agent must complete and sign the appropriate form.
- 16.3 Similarly, a surveillance authorisation should also be considered where the Council is aware that a third party (that is not a public Authority) is independently conducting surveillance and the Council intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation or is to act as the prosecuting body.

17. EQUIPMENT

- 17.1 All equipment capable of being used for directed surveillance, such as cameras, should be fit for the purpose for which they are intended. The equipment should be logged on the central register of equipment held by the RIPA Coordinator. This will require a description, Serial Number, and an explanation of its capabilities.
- 17.2 When completing an Authorisation, the applicant must provide the AO with details of any equipment to be used and its technical capabilities. The AO will have to take this into account when considering the intrusion issues and proportionality. The AO must make it clear on the Authorisation exactly what equipment, if any, they are authorising and under what circumstances.

18. COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

- 18.1 This policy applies to all use of under-cover Officers or informants, referred to as Covert Human Intelligence Sources (CHIS). Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of a professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship.
- 18.2 Test purchase activity does not in general require authorisation under RIPA as vendor-purchaser activity does not constitute a relationship. However, if a number of visits are undertaken, a relationship may be established and

authorisation as a CHIS should be considered. Equally a test purchase may meet the definition of directed surveillance.

- 18.3 If you intend to instruct a third party to act as the CHIS, the agent must complete and sign the appropriate form. The agent will be subject to RIPA in the same way as any employee of the Council would be. If advice is required, please contact either the RIPA Coordinator or the Legal Department.
- 18.4 An application for either directed surveillance or the use of a CHIS will need authorising internally by an AO. If authorised by the AO, approval will be required from a Justice of the Peace (JP) prior to any activity taking place. (See the appropriate sections below).
- 18.5 The authorisation request should be accompanied by a risk assessment, giving details of how the CHIS is going to be handled and the arrangements which are in place for ensuring that there is at all times a person with responsibility for maintaining a record of the use made of CHIS. The risk assessment should take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.
- 18.6 Where surveillance or the use of a CHIS is likely to result in the obtaining of confidential information, it is imperative that legal advice should first be sought from the SRO or the Legal Department. Confidential information includes, though is not limited to, matters subject to legal privilege, confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it.
- 18.7 Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice.
- 18.8 Legal advice should always be sought where consideration is given to the use of CHIS.
- 18.9 DEFINITION OF CHIS
- 18.10 A CHIS is a person who: -
- Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the following paragraphs;
 - Covertly uses such a relationship to obtain information or to provide access to any information to another person; or
 - Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.
- 18.11 A relationship is established, maintained or used 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.
- 18.12 The serious crime criteria of the offences under investigation do not apply to CHIS.
- 18.13 CHIS's may only be authorised if the following arrangements are in place:

- That there will at all times be an Officer (the handler) 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 is likely to be the IO,
- 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 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.
- That the records relating to the source maintained by the local authority will always contain particulars of all matters specified by the Secretary of State in Regulations.

18.14 The Handler will have day to day responsibility for:

- dealing with the source on behalf of the Council concerned;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare.

18.15 The Controller will be responsible for the general oversight of the use of the source.

18.16 Tasking is the assignment given to the source by the Handler or Controller such as asking them to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant Council. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

18.17 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a member of the public is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

18.18 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task.

18.19 VULNERABLE CHIS

18.20 Special consideration must be given to the use of a Vulnerable Individual as a 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 Senior Responsible Officer.

- 18.21 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 them.
- 18.22 If the use of a Vulnerable Individual or a Juvenile is being considered as a CHIS you must consult the Legal Department before authorisation is sought as 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 must be authorised by the Senior Responsible Officer within the Council.
- 18.23 It is unlikely that the use of a Vulnerable Individual or Juvenile CHIS by the Council will meet the requirements of necessity and proportionality and be considered justifiable.
- 18.24 USE OF EQUIPMENT BY A CHIS
- 18.25 If a CHIS is required to wear or carry a surveillance device such as a covert camera it does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. It should be authorised as part of the conduct of the CHIS.
- 18.26 CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations.
- 18.27 CHIS MANAGEMENT
- 18.28 The operation will require managing by the handler and controller which will include ensuring that the activities of the source and the operation remain focused and there is no status drift. It is important that the intrusion is assessed on an ongoing basis to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The AO should maintain general oversight of these functions.
- 18.29 During CHIS activity there may be occasions when unforeseen action or undertakings occur. Such incidences should be recorded as soon as practicable after the event and if the existing authorisation is insufficient, it should either be dealt with by way of a review and re-authorisation (for minor amendments only) or it should be cancelled, and a new authorisation obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking should be referred to the AO, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and details of such referrals must be recorded.
- 18.30 CHIS RECORD KEEPING
- 18.31 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, revised CHIS codes of practice and the RIPA (Source Records) Regulations 2000; SI No: 2725 which details the particulars that must be included in these records.

19. NECESSITY

- 19.1 Obtaining an authorisation under RIPA 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.
- 19.2 RIPA 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 applicable to the Council.
- 19.3 The applicant must be able to demonstrate why it is necessary to carry out the covert activity to achieve the objectives and that there was no other means of obtaining the same information in a less intrusive method. The applicant must detail the crime being investigated and the information or evidence they are hoping to obtain. They should also state that they have considered other means of obtaining this information and have either concluded this is the only method available or that other methods are not appropriate and state the reason; for example it would alert the subject to their investigation which would be detrimental to the case.

20. PROPORTIONALITY

- 20.1 If the activities are deemed necessary, the AO must also believe that they are proportionate to the objective they are aiming to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.
- 20.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.
- 20.3 When completing the authorisation the AO should explain why the methods and tactics to be adopted during the surveillance are justified in the particular circumstances of the case.
- 20.4 The Codes provide guidance relating to proportionality which should be considered by both applicants and AOs:
- 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.
- 20.5 When completing an application for authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

21. COLLATERAL INTRUSION

- 21.1 Before authorising applications for directed surveillance, the AO should also take into account the risk of collateral intrusion - obtaining private information about persons who are not subjects of the surveillance.
- 21.2 Officers should take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to the aims of the operation. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.
- 21.3 All applications must include an assessment of the risk of collateral intrusion and details of any measures taken to limit this (within the relevant section of the form), to enable the AO to fully consider the proportionality of the proposed actions.
- 21.4 In order to give proper consideration to collateral intrusion, an AO should be given full information regarding the potential scope of the anticipated surveillance, including the likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the AO should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. The AO should ensure appropriate safeguards for the handling, retention or destruction of such material, as well as compliance with Data Protection Act requirements.
- 21.5 Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but rather as intended intrusion.
- 21.6 Where the Council intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a Directed Surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

22. THE APPLICATION AND AUTHORISATION PROCESS

- 22.1 All forms relating to RIPA can be found at <https://www.gov.uk/government/collections/ripa-forms--2>
- 22.2 DURATION OF AUTHORISATIONS
- 22.3 Authorisations must be given for the maximum duration from the date approved by the JP/Magistrate but reviewed on a regular basis and formally cancelled when no longer needed. They do not expire – they must be cancelled when the surveillance is no longer proportionate or necessary. Therefore, a directed surveillance authorisation will cease to have effect after three months from the date of approval by the Magistrate unless renewed or cancelled. Durations detailed below:

- Directed Surveillance 3 Months
- Renewal 3 Months
- Covert Human Intelligence Source 12 Months
- Renewal 12 months
- Juvenile Sources 4 Months
- Renewal 4 Months

22.4 It is the responsibility of the IO to make sure that the authorisation is still valid when they undertake surveillance.

22.5 APPLICATIONS/AUTHORISATION

22.6 The applicant or some other person must carry out a feasibility study and intrusion assessment as this may be required by the AO. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application remain accurate. The form should then be submitted to the AO for authorisation.

22.7 When completing an application, the applicant must ensure that the case for the authorisation is presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation.

22.8 For directed surveillance, the offence must be a criminal offence that attracts 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.

22.9 All the relevant sections must be completed with enough information to ensure that applications are sufficiently detailed for the AO to consider necessity and proportionality, having taken into account the collateral intrusion issues. AOs should refuse to authorise applications that are not to the required standard and should refer them back to the originating Officers. Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.

22.10 If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective application form and procedures should be followed, and both activities should be considered separately on their own merits.

22.11 All applications will be submitted to the AO via the Line Manager of the appropriate enforcement team in order that they are aware of the application and activities being undertaken by their 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.

22.12 Applications, whether authorised or refused, will be issued with a unique number (obtained from the RIPA Coordinator) by the AO, taken from the next available number in the central record of authorisations which is held by the RIPA Coordinator.

22.13 If not authorised, feedback will be provided to the applicant and the application will be forwarded to the RIPA Coordinator for recording and filing.

22.14 If authorised, the applicant will then complete the relevant section of the judicial application/order form. Although this form requires the applicant to provide a

brief summary of the circumstances of the case, this is supplementary and does not replace the need to supply the original RIPA authorisation form to the Court.

22.15 ARRANGING THE COURT HEARING

22.16 Within office hours a hearing must be arranged at the Magistrates' Court with Her Majesty's Courts and Tribunals Service (HMCTS). The hearing will be in private and heard by a single JP. The application to the JP will be on oath.

22.17 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 information as required by the JP. The legal department can advise who is duly authorised and able to present.

22.18 ATTENDING THE HEARING

22.19 The applicant and the AO should attend the Hearing to answer any questions directed at them. Upon attending the hearing, the presenting Officer must provide to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, and the original form, together with any supporting documents setting out the case.

22.20 The original RIPA authorisation should be shown to the JP but will be retained by the Council so that it is available for inspection by IPCO, and in the event of any legal challenge or investigations by the IPT.

22.21 The JP will read and consider the RIPA authorisation and the judicial application/order form. They may ask questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form. The forms and supporting papers must by themselves make the Council's case. It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided.

22.22 The JP will consider whether they are satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. 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.

22.23 DECISION OF THE JP

22.24 The JP has a number of options:

22.25 Approve or renew an authorisation. 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.

22.26 Refuse to approve or renew an authorisation. The RIPA authorisation will not take effect and the Council may **not** use the technique in that case.

22.27 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 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.

22.28 For, a technical error (as defined by the JP), 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.

22.29 Refuse to approve or renew and quash the authorisation. This applies where the JP refuses to approve or renew the authorisation and decides to quash the original authorisation. However, the court must not exercise its power to quash the authorisation unless the applicant has had at least two business days from the date of the refusal in which to make representations. If this is the case the Officer will inform the Legal Department who will consider whether to make any representations.

22.30 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 authorisation and a copy of the judicial application/order form.

22.31 The Council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal Department will decide what action if any should be taken.

22.32 POST COURT PROCEDURE

22.33 It will be necessary to work out the cancellation date from the date of approval and ensure that the applicant and the AO are aware. The original application and the copy of the judicial application/order form should be forwarded to the RIPA Coordinator. A copy will be retained by the applicant and if necessary by the AO. The Central Register of Authorisations will be updated with the relevant information to comply with the Codes of Practice and the original documents filed and stored securely.

22.34 Where dates are set within the process such as reviews, they must be adhered to. This will help with demonstrating that the process has been managed correctly in line with the Codes of Practice.

22.35 MANAGEMENT OF THE ACTIVITY

22.36 All RIPA activity will need to be managed by all the persons involved in the process. It is important that all those involved in undertaking directed surveillance activities are fully aware of the extent and limits of the authorisation. There should be an ongoing assessment of the need for the continued activity, including ongoing assessments of the intrusion. All material obtained including evidence should be stored in line with relevant legislation and procedures to safeguard its integrity and reduce a risk of challenge. (See use of material as evidence)

22.37 REVIEWS

22.38 When an application has been authorised and approved by a JP, regular reviews must be undertaken by the AO to assess the need for the surveillance to continue.

22.39 In each case the AO should determine at the outset how often a review should take place. This should be as frequently as is considered necessary and

practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides a high level of intrusion into private life or significant collateral intrusion, or may obtain confidential information. Review periods will be recorded on the application form and the decision will be based on the circumstances of each application. However, reviews should be conducted at least monthly to ensure that the activity is managed. It will be important for the AO to be aware of when reviews are required following an authorisation, to ensure timely submission of the review form.

- 22.40 Applicants are responsible for submitting a review form by the date set by the AO. They should also use a review form for any changes in circumstances to the original application which would comprise a change to the level of intrusion so that the requirement to continue the activity can be reassessed. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances. If the circumstances or the objectives have changed considerably, or the techniques to be used are now different, a new RIPA application form should be submitted and the process followed to obtain approval by a JP.
- 22.41 Line managers should also make themselves aware of the required review periods to ensure that the relevant forms are completed on time.
- 22.42 The reviews are dealt with internally by submitting the review form to the AO. There is no requirement for a review form to be submitted to a JP.
- 22.43 The results of a review should be recorded on the Central Record of Authorisations.
- 22.44 RENEWAL
- 22.45 A renewal form is to be completed by the applicant when the original authorisation period is about to expire but directed surveillance or the use of a CHIS is still required.
- 22.46 Renewals must be approved by a JP.
- 22.47 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 AO and a JP to consider the application).
- 22.48 The applicant should complete all the sections within the renewal form and submit the form to the AO for consideration.
- 22.49 AOs should examine the circumstances with regard to necessity, proportionality and the collateral intrusion 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 AO must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.
- 22.50 If the AO 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 for the initial application whereby approval must be sought from a JP.
- 22.51 A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

22.52 CANCELLATION

- 22.53 The cancellation form is to be submitted by the applicant or another investigator in their absence. The AO 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 AO is no longer available, this duty will fall on the person who has taken over the role of AO or the person who is acting as AO.
- 22.54 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other IO involved in the investigation should inform the AO. The AO will formally instruct the IO 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.
- 22.55 The IO submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and also detail if any images were obtained, particularly any images containing third parties. The AO should then take this into account and issue instructions regarding the management and disposal of the images. See section below; Safeguarding and the Use of Surveillance Material.
- 22.56 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant acted within the authorisation. 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 SRO.
- 22.57 When cancelling a CHIS authorisation an assessment of the welfare and safety of the source should be assessed, and any issues identified and reported as above.

23. SURVEILLANCE OUTSIDE OF RIPA

- 23.1 As previously detailed, amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that Councils can now only grant an authorisation under RIPA where the Council 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.
- 23.2 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 disorders which do not attract a maximum custodial sentence of at least six months imprisonment).
- 23.3 As stated, conducting surveillance outside of RIPA is not fundamentally unlawful, however in order for the Council to defend claims that they have breached an individual's right to privacy under the HRA the Council needs to demonstrate that their actions were justified in the circumstances of the case. It is therefore the Council's policy that, in order to undertake surveillance that falls outside of RIPA, Officers will follow the same initial process as when they are making an application for authorisation under RIPA. The IO must complete a Non-RIPA application form that is authorised by an AO and the application will be lodged with and monitored by the RIPA Coordinator. The AO will need to be satisfied that the actions are necessary and proportionate and give due consideration to any collateral intrusion. The Non-RIPA authorisation form is available from the RIPA Coordinator. The procedure for review and renewal of the surveillance

application will be the same, however there is no requirement/ability to obtain authorisation from a JP.

23.4 Non-RIPA surveillance also includes staff surveillance in serious disciplinary investigations. Any surveillance of staff must be formally recorded on the Non-RIPA surveillance application form and authorised by the AO in consultation with the RIPA Coordinator. The review of staff usage of the internet and e-mail would also not fall under RIPA. This surveillance outside of RIPA must however be compliant with any Council Policies with regard to monitoring at work and business practices legislation and should also consider ICO guidance in relation to surveillance of staff. Surveillance of staff should only be carried out in exceptional circumstances.

23.5 The RIPA codes also provide guidance that authorisation under RIPA is not required for the following types of activity:

- General observations that do not involve the systematic surveillance of an individual or a group of people and should an incident be witnessed the Officer will overtly respond to the situation.
- Use of overt CCTV and Automatic Number Plate Recognition systems.
- Surveillance where no private information is likely to be obtained.
- Surveillance undertaken as an immediate response to a situation.
- Covert surveillance not relating to criminal offence which carries a maximum sentence of 6 months imprisonment and does not relate to the sale of alcohol or tobacco to children (surveillance outside of RIPA).
- The use of a recording device by a CHIS in respect of whom an appropriate use or conduct authorisation has been granted permitting them to record any information in their presence.
- The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance this is outside of RIPA.

24. SAFEGUARDING AND THE USE OF SURVEILLANCE MATERIAL

24.1 This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through directed surveillance or CHIS activity. This material may include private, confidential or legally privileged information.

24.2 AUTHORISED PURPOSE

24.3 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of this Code this is defined as follows:-

- It is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA in relation to covert surveillance or CHIS activity;
- It is necessary for facilitating the carrying out of the functions of public authorities under RIPA;

- It is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- It is necessary for the purposes of legal proceedings; or
- It is necessary for the performance of the functions of any person by or under any enactment.

24.1 USE OF MATERIAL AS EVIDENCE

24.2 Material obtained through directed surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996 (CPIA), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

24.3 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the CPIA and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the Council must be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

24.4 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In a criminal case the codes issued under CPIA will apply. They require that the investigator record and retain all relevant material obtained in an investigation and later disclose relevant material to the prosecuting solicitor. They in turn will decide what is disclosed to the defence solicitor.

24.5 There is nothing in RIPA which prevents material obtained under directed or intrusive surveillance authorisations from being used to further other investigations.

24.6 HANDLING AND RETENTION OF MATERIAL

24.7 All material associated and obtained with an application will be subject to the provisions of all data protection legislation and regulations and CPIA Codes of Practice and to any Council Policies with regard to data retention and security. All Officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the RIPA process. Material obtained together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

24.8 Material required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

24.9 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

24.10 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material

which may be relevant must be retained at least until six months from the date of conviction.

- 24.11 If an appeal against conviction is in progress when the convicted person is released, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.
- 24.12 Retention beyond these periods must be justified under data protection legislation and regulations. AOs, through the Council's Data Controller, must ensure compliance with the appropriate Data Protection requirements and any relevant internal arrangements produced by the Council relating to the handling and storage of material.
- 24.13 DISSEMINATION OF INFORMATION
- 24.14 It may be necessary to disseminate material acquired through the RIPA covert activity within the Council or with other Councils or agencies, including the Police. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.
- 24.15 The obligations apply not just to the Council as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from the Council before disclosing the material further. It is important that the Officer in Charge (OIC) of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.
- 24.16 A record will be maintained justifying any dissemination of material. If in doubt, seek legal advice.
- 24.17 STORAGE
- 24.18 Material obtained through covert surveillance, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss. It must be held so as to be inaccessible to persons who are not required to see the material (where applicable). This requirement applies to all those who are responsible for the handling of the material. It will be necessary to ensure that an appropriate security clearance regime is in place to safeguard the material whether held electronically or physically.
- 24.19 COPYING
- 24.20 Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.
- 24.21 In the course of an investigation, the Council must not act on or further disseminate legally privileged items unless it has first informed the IPC that the items have been obtained.

24.22 DESTRUCTION

24.23 Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

25. ERRORS

25.1 Proper application of the surveillance provisions in the RIPA codes and this Policy should reduce the scope for making errors.

25.2 RELEVANT ERROR

25.3 An error must be reported if it is a “**relevant error**”. A relevant error is any error by the Council in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of RIPA.

25.4 Examples of relevant errors occurring would include circumstances where:

- Surveillance activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

25.5 Errors can have very significant consequences on an affected individual's rights. All relevant errors made by the Council must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and a full report no later than ten working days after the error is discovered. The report should include information on the cause of the error; the amount of surveillance conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

25.6 SERIOUS ERRORS

25.7 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a **serious error** and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's convention rights (within the meaning of the HRA) is not sufficient by itself for an error to be a serious error.

25.8 It is important that all staff involved in the RIPA process report any issues, so they can be assessed as to whether it constitutes an error which requires reporting.

26. COMPLAINTS

- 26.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against the Council's use of investigatory powers, including those covered by this code. Any complaints about the use of powers as described in this code should be directed to the IPT.
- 26.2 Complaints should be addressed to:
The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

| | |
|-----------------------------|---|
| Version Control: | |
| Document Name: | Investigatory Powers Act 2016 Acquisition of Communications Data Policy |
| Version: | 1 |
| Responsible Officer: | Emma Cathcart, Counter Fraud Unit |
| Approved by: | Cabinet |
| Date First Approved: | |
| Next Review Date | |
| Retention Period: | N/A |

Revision History

| Revision date | Version | Description |
|---------------|---------|--|
| April 2019 | 1 | Change in legislation / introduction of IPA 2016 |
| | | |

Consultees

| Internal | External |
|----------------------|----------|
| Audit Committee | |
| Legal Department | |
| Corporate Management | |

Distribution

| Name | |
|----------------------|--|
| Enforcement Officers | |
| | |

CONTENTS

| | | |
|-----|---|----|
| 1. | INTRODUCTION | 4 |
| 2. | SCOPE OF POLICY | 4 |
| 3. | ROLES OF STAFF INVOLVED IN THE PROCESS..... | 4 |
| 4. | APPLICANT..... | 5 |
| 5. | DESIGNATED PERSON | 5 |
| 6. | SINGLE POINT OF CONTACT..... | 5 |
| 7. | OCDA AUTHORISING INDIVIDUAL..... | 6 |
| 8. | WHAT IS COMMUNICATIONS DATA | 6 |
| 9. | COMMUNICATIONS DATA DEFINITIONS..... | 6 |
| 10. | POSTAL DEFINITIONS | 7 |
| 11. | WEB BROWSING AND COMMUNICATIONS DATA..... | 8 |
| 12. | RELEVANT COMMUNICATIONS DATA | 8 |
| 13. | INTERNET CONNECTION RECORDS | 9 |
| 14. | PREPAID MOBILE PHONES..... | 9 |
| 15. | WHO CAN COMMUNICATIONS DATA BE OBTAINED FROM? | 9 |
| 16. | LAWFUL REASONS TO ACCESS COMMUNICATIONS DATA | 10 |
| 17. | USING OTHER POWERS | 10 |
| 18. | INTERNAL INVESTIGATIONS | 10 |
| 19. | SERIOUS CRIME THRESHOLD | 10 |
| 20. | NECESSITY AND PROPORTIONALITY | 11 |
| 21. | NECESSITY | 11 |
| 22. | PROPORTIONALITY..... | 11 |
| 23. | COLLATERAL INTRUSION | 12 |
| 24. | THE TWO WAYS OF OBTAINING COMMUNICATIONS DATA | 12 |
| 25. | THE APPLICATION PROCESS..... | 13 |
| 26. | TIME SCALES..... | 14 |
| 27. | APPLICATION FORM..... | 14 |
| 28. | URGENT ORAL AUTHORISATION..... | 15 |
| 29. | ERRORS | 15 |
| 30. | REPORTABLE ERROR..... | 16 |
| 31. | RECORDABLE ERROR | 16 |
| 32. | EXCESS DATA..... | 16 |
| 33. | RECORD KEEPING AND SECURITY OF DATA..... | 17 |
| 34. | CRIMINAL PROCEDURES AND INVESTIGATIONS ACT (CPIA) | 17 |
| 35. | DATA PROTECTION ACT 2018 (DPA) AND THE GENERAL DATA PROTECTION REGULATIONS (GDPR) | 18 |

36. OVERSIGHT..... 18

37. COMPLAINTS 19

38. STRATEGY AND POLICY REVIEW 19

1. INTRODUCTION

- 1.1. The Investigatory Powers Act 2016 (IPA) governs how law enforcement agencies use the investigatory powers available to them, in relation to the lawful acquisition of Communications Data (CD). The IPA provides unprecedented transparency and substantial privacy protection, strengthening safeguards and introducing oversight arrangements. It also introduces a powerful new Investigatory Powers Commission (IPC) to oversee how these powers are used.
- 1.2. The powers provided by the Regulation of Investigatory Powers Act 2000 (RIPA) allowed the Council to obtain CD from Communications Service Providers (CSPs) in connection with criminal investigations.
- 1.3. The IPA extends the range of data Councils are able to request from providers but ensures independent authorisation for the acquisition through the new Office for Communications Data Authorisations (OCDA). However, it continues only to be a justifiable interference with an individual's human rights if such conduct is authorised, is both necessary and proportionate, and is in accordance with the law.
- 1.4. All applications for CD must be made via an Accredited Officer known as a Single Point of Contact (SPoC) who has passed a Home Office approved course. All Councils must use the National Anti-Fraud Network (NAFN) as their SPoC. Therefore, all applications to access CD will be made through NAFN via their online application service.
- 1.5. The introduction of OCDA means the acquisition of CD by Council officers no longer requires judicial approval.
- 1.6. These powers should not be confused with any Policy and practices with regard to monitoring under the lawful business practices legislation. This latter legislation relates to the monitoring of the Council's own communication and computer systems.

2. SCOPE OF POLICY

- 2.1. This Policy sets out the Council's procedures and approach for obtaining and handling CD for the purposes of preventing or detecting crime or of preventing disorder; the only lawful reasons for Council staff to use IPA legislation to access CD.
- 2.2. This Policy should be read in conjunction with the Communications Data Code of Practice (COP), currently in draft. This also creates a system of safeguards, consistent with the requirements of Article 8 (rights to privacy) of the Human Rights Act 1998. The Codes of Practice are admissible in evidence in criminal and civil proceedings.
- 2.3. The draft Code can be obtained using the link detailed below and is available to all Council staff involved in the acquisition of CD.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757851/Communications_Data_Code_of_Practice.pdf
- 2.4. Both this Policy and the COP will be followed at all times and under no circumstances should access to CD be sought outside of this guidance.
- 2.5. The Council will review and amend this Policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the objectives of the Council.

3. ROLES OF STAFF INVOLVED IN THE PROCESS

- 3.1. The process for the acquisition of CD under the IPA requires the following personnel:

- Applicant
- Designated Person (DP)
- Single Point of Contact (SPoC)
- OCDA Authorising Individual

4. APPLICANT

- 4.1. The Applicant is a person involved in conducting an investigation or operation who makes an application in writing for the acquisition of CD. The Applicant completes an application form, setting out for consideration the necessity and proportionality of a specific requirement for acquiring CD. Prior to the completion of the relevant paperwork, it may be advisable for the Applicant to consult with the SPoC at NAFN.

5. DESIGNATED PERSON

- 5.1. The DP is a person of Service Manager level or equivalent within the Council who confirms to NAFN that they are aware that an application has been made. They do not have any authorising function but are responsible for the integrity of the process in place and the overall quality of that process.

6. SINGLE POINT OF CONTACT

- 6.1. The SPoC is either an accredited individual (passed the Home Office course) or a group of accredited individuals such as the National Anti-Fraud Network, who are trained to facilitate lawful acquisition of CD. All accredited officers are issued a Personal Identification Number (PIN). Details of all accredited individuals are available to Communication Service Providers (CSPs) for authentication purposes.
- 6.2. An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for CD are undertaken. The SPoC provides objective judgement and advice to the Applicant and provides a "guardian and gatekeeper" function, ensuring that public authorities act in an informed and lawful manner.
- 6.3. As already explained, this Council can only use the services of NAFN as the Council's SPoC. Therefore, all applications to access CD will be made through NAFN.
- 6.4. The SPoC will be in a position to:
- Engage proactively with Applicants to develop strategies to obtain CD and use it effectively in support of operations or investigations;
 - Assess whether the acquisition of specific CD from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;
 - Advise Applicants on the most appropriate method for the acquisition of data where the data sought engages a number of CSPs;
 - Advise Applicants on the type of data that can be obtained to meet their purposes.
 - Provide assurance to DPs that Authorisations and Notices are lawful under the IPA and free from errors;
 - Provide assurance to OCDA that an application has been verified and checked.

- Assess whether CD disclosed by a CSP in response to a Notice fulfils the requirement of the Notice;
- Assess whether CD obtained by means of an Authorisation fulfils the requirement of the Authorisation;
- Assess any cost and resource implications to both the Council and the CSP of data requirements.

7. OCDA AUTHORISING INDIVIDUAL

- 7.1. The OCDA officer receives the application from the NAFN SPoC and checks the application meets the necessary criteria before authorising or rejecting and issuing a Decision Document. NAFN will retain the original of all the documents. These will be retained within the on-line portal. Copies of the documents must be retained by the Applicant, DP or within the relevant department for inspection by the IPC and for audit, filing and disclosure purposes under the Criminal Procedures Investigation Act 1996. (OCDA will only hold the applications and Decision Documents for a limited period of time due to the degree of sensitivity and risk arising from the accumulation of these documents in a central database.)

8. WHAT IS COMMUNICATIONS DATA

- 8.1. CD does not include the content of any communication. It is not lawfully possible for Council employees under any circumstances to obtain the content of communications.
- 8.2. The term 'CD' embraces the 'who', 'when' and 'where' of a communication but not the content - not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video
- 8.3. CD can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.
- 8.4. CD is generated, held or obtained in the provision, delivery and maintenance of communications services – i.e. postal services or telecommunications services.
- 8.5. Where the provision of a communication service engages a number of providers, the SPoC will determine the most appropriate plan for acquiring the data.
- 8.6. When enquiries regarding CD are being considered within an investigation, it may be advisable that Applicants seek advice and guidance from the SPoC at NAFN. The RIPA Coordinator /DP within the Counter Fraud Unit can provide contact details.

9. COMMUNICATIONS DATA DEFINITIONS

- 9.1. The IPA introduces new terminology for CD – Entity Data and Events Data
- 9.2. Entity Data describes the 'who' involved in the communication – the subscriber and the links between different entities or communicators. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).
- 9.3. Examples of entity data requests include:

- Subscriber checks, such as who is the subscriber of phone number 01234 567 890?
- Who is the account holder of e-mail account example@example.co.uk?
- Who is entitled to post to web space www.example.co.uk?
- Subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments e.g. for pre-paid mobiles.
- Information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services.
- Information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes.
- Information about selection of preferential numbers or discount calls.

9.4. Event Data identifies or describes events in relation to a telecommunications system which consists of one or more entities engaging in an activity at a specific point or points in time – the 'what, when and where'. For obtaining Event Data there is a Serious Crime Threshold (see 11.1)

9.5. Examples of events data include, but are not limited to:

- Information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- Information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- Information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- Routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- Itemised telephone call records (numbers called)¹²;
- Itemised internet connection records;
- Itemised timing and duration of service usage (calls and/or connections);
- Information about amounts of data downloaded and/or uploaded;
- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

10. POSTAL DEFINITIONS

10.1. A postal service is a service which involves one or more of the collection, sorting, conveyance, distribution and delivery of postal items and where its main purpose is to

make available or facilitate the transmission of postal items containing communications. CD in relation to a postal service is defined at section 262(3) of the IPA and comprises three elements:

- Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted;
- Data relating to use made by a person of a postal service;
- Information held or obtained by a postal operator about persons to whom the postal operator provides or has provided a communications service and which relates to the provision of the service.

10.2. Postal data is defined in section 262(4) of the IPA and includes specified categories of data written on the outside of a postal item. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is postal data.

10.3. In the postal context anything included inside a postal item, which is in transmission, will be content. Any message written on the outside of a postal item which is in transmission may be content and fall within the scope for the interception of communications. For example, a message written by the sender for the recipient will be content but a message written by a postal worker concerning the delivery of the postal item will not. All information on the outside of a postal item concerning its routing, for example the address of the recipient, the sender and the postmark, is postal data and will not be content.

11. WEB BROWSING AND COMMUNICATIONS DATA

11.1. Web browser software provides one way for users to access web content. When using a browser to access the web, a user may enter a web address. These are also referred to as uniform resource locators (URLs).

11.2. Some elements of a URL are necessary to route a communication to the intended recipient and are therefore CD. The URL may also contain the port, which is an extended part of the Internet Provider (IP) address and the user information – including usernames and authorisations. The port and user information will be CD.

12. RELEVANT COMMUNICATIONS DATA

12.1. A data retention notice under the IPA may only require the retention of relevant CD. This is defined at section 87 of the IPAt and is a subset of CD.

It is data which may be used to identify or assist in identifying any of the following:

- The sender or recipient of a communication;
- The time or duration of a communication;
- The type, method or pattern, or fact of a communication;
- The telecommunication system to or through which a communication is transmitted;
- The location of any such system.

13. INTERNET CONNECTION RECORDS

- 13.1. An internet connection record (ICR) is a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet. An ICR is CD.
- 13.2. An ICR will only identify the service that a customer has been using. For example many social networking apps on a device maintain persistent connections to a service. Even in this case the relevant ICR will signpost the service accessed by the device, enabling the authority to make further enquiries of the social networking provider identified.
- 13.3. Further detail on the definitions described above and the types of CD that can be accessed is available in the COP.
- 13.4. The SPoC will provide advice and assistance with regard to the types of data which can be lawfully obtained and how that data may assist an investigation. Where an applicant is unsure of the category of data they are seeking (entity or events data) or what additional types of CD may be retained by a telecommunications operator or postal operator for their own business use, the applicant should discuss this with their Single Point of Contact (SPoC).

14. PREPAID MOBILE PHONES

- 14.1. Unregistered prepaid mobile phones are common amongst criminals as it allows them to avoid detection more easily. It is 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. The Applicant can ask for further information about the subscriber under section 21(4)(c), including top-up details, method of payment, the bank account used or customer notes etc.
- 14.2. So as to allow for the widening of the data capture, the Applicant should outline in their original application that further information will be required if the phone turns out to be prepaid, 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.
- 14.3. 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 the IPA; instead the data can be applied for under the Data Protection Act via the SPoC.

15. WHO CAN COMMUNICATIONS DATA BE OBTAINED FROM?

- 15.1. CD can be obtained from a Communications Service Provider (CSP). A CSP is an operator who provides a postal service such as Royal Mail or telecommunications service, such as the usual telephone service providers. However, there may be less obvious companies which may be classed as a CSP. The SPoC at NAFN will determine which CSP they will contact to obtain the data on behalf of the Applicant. However, any intelligence obtained which establishes which CSP may provide the data should be included within the application or by notifying the SPoC.

16. LAWFUL REASONS TO ACCESS COMMUNICATIONS DATA

- 16.1. As mentioned earlier the Council's only lawful reasons to access CD is for the purpose of preventing or detecting crime or of preventing disorder.
- 16.2. Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.
- 16.3. The Council can only lawfully process and consider applications to access CD on behalf of the Council. Under no circumstances will applications be accepted for outside authorities/agencies. However, it may be necessary during joint investigations to obtain CD; in these circumstances the Council can only apply for data which it would usually be allowed to access. It should be clear in the investigation Policy log that it is a joint investigation as it may have to be justified to a Court or Tribunal.
- 16.4. Staff must not apply on behalf of any third parties who do not have lawful authority to obtain CD. Should an organisation make such an approach this must be reported to the Senior Responsible Officer (SRO) who has the responsibility for the Council's working practices in relation to obtaining CD.
- 16.5. Where the Council is contracted to undertake work on behalf of a third party, CD may be obtained if the Council is the investigating and prosecuting body.

17. USING OTHER POWERS

- 17.1. The IPA is the primary legislation for the acquisition of CD and should always be the first option considered due to the rigorous and independent assessment and authorisation process.

18. INTERNAL INVESTIGATIONS

- 18.1. The Codes state 'where an investigation relates to an allegation of criminal conduct by a member of a public authority, that public authority (or another public authority appointed to investigate the complaint) may use their powers under Chapter II to obtain CD for the purpose of preventing and detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain CD under the Act'.
- 18.2. If CD is sought in connection with officers of the Council committing crimes against the Council, it is important that the enquiry is a genuine criminal investigation with a view to proceeding criminally as opposed to just a disciplinary matter. Advice may be required from the Council's Legal section if this arises.

19. SERIOUS CRIME THRESHOLD

- 19.1. With effect from 1st November 2018 the IPA introduced a new Serious Crime Threshold to applications for CD. This means the Council may only acquire Events Data where the crime can be defined as a serious crime. Where the crime cannot be defined as serious, only Entity Data may be obtained.
- 19.2. The following definitions of serious crime apply:

- An offence that is capable of attracting a prison sentence of 12 months or more;
- An offence by a person who is not an individual (i.e. a corporate body);
- An offence falling within the definition of serious crime in section 263(1) of the IPA (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose);
- An offence which involves, as an integral part of it, the sending of a communication;
- An offence which involves, as an integral part of it a breach of a person's privacy.

20. **NECESSITY AND PROPORTIONALITY**

- 20.1. The COP states the acquisition of CD under the IPA will be a justifiable interference with an individual's human rights under Article 8 Right to Privacy, only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.
- 20.2. Below is guidance to assist Applicants with factors that impact on necessity and proportionality.

21. **NECESSITY**

- 21.1. In order to justify the application is necessary, the Applicant needs as a minimum to consider three main points:
1. The event under investigation, such as a crime or disorder offence;
 2. The person, such as a suspect, witness or missing person and how they are linked to the event;
 3. The Communication Data, such as a telephone number or IP address, and how this data is related to the person and the event.
- 21.2. In essence, necessity should be a short explanation of **1) the event, 2) the person and 3) the CD and how these three link together**. The application must establish a link between the three aspects to be able to demonstrate the acquisition of CD is necessary for the statutory purpose specified.
- 21.3. 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.

22. **PROPORTIONALITY**

- 22.1. 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.
- 22.2. This outline should include an explanation of 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 online enquiries or other publicly available sources.

- 22.3. 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?
- 22.4. Particular consideration should be given to any periods of days or shorter periods of time which might achieve the objective. They should specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise will impact on the proportionality of the Authorisation or Notice and impose unnecessary burden upon a CSP.
- 22.5. An explanation as to how CD once acquired will be used, and how it will benefit the investigation or operation will enable the Applicant to set out the basis of proportionality.
- 22.6. 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.
- 22.7. 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.

23. COLLATERAL INTRUSION

- 23.1 Consideration of collateral intrusion forms part of the proportionality considerations and becomes increasingly relevant when applying for Events Data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion.
- 23.2 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.
- 23.3 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'.
- 23.4 It is accepted that for a straight forward subscriber check there will be no meaningful collateral intrusion.

24. THE TWO WAYS OF OBTAINING COMMUNICATIONS DATA

- 24.1. The legislation provides two different methods of acquiring CD (see below). The SPoC at NAFN will be responsible for deciding the process for obtaining the data required and passing responses from the service provider to the Council.
- 24.2. The two methods are:

- **Authorisation of conduct, or**
- **Authorisation to give a Notice**

24.3. An authorisation of conduct to acquire CD may be appropriate where, for example:

- there is an agreement in place between a public authority and a telecommunications operator or postal operator to facilitate the secure and swift disclosure of CD. Many telecommunications operators and postal operators have auditable acquisition systems in place to ensure accurate and timely acquisition of CD, while maintaining security and an audit trail;
- where the data can be acquired directly from a telecommunication system and the activity does not constitute interception or equipment interference; or
- a public authority considers there is a requirement to identify a person to whom a service is provided but the specific telecommunications operator or postal operator has yet to be conclusively determined as the holder of the CD.

An authorisation to give a notice may be appropriate where a telecommunications operator or postal operator is known to be capable of disclosing (and, where necessary, obtaining) the CD

25. THE APPLICATION PROCESS

25.1. From April 2019 the IPA removes the requirement to obtain judicial approval. Applications will only require Independent Authorisation.

25.2. Prior to an Applicant applying for CD, they should contact a SPoC at NAFN who will be in a position to advise them regarding the obtaining and use of CD within their investigation. This will reduce the risk of the Applicant applying for data which they are not able to obtain. It will also assist the Applicant to determine their objectives and apply for the most suitable data for those circumstances.

25.3. The Council will use the automated application process provided by NAFN. This automated service contains the relevant documentation for the Applicant to complete the relevant forms.

25.4. To use the system, Applicants and the DP have to individually register on the NAFN website - www.nafn.gov.uk. A number of departments within the Council have contributed towards the NAFN annual membership fee; therefore an Applicant needs to confirm with their Line Manager that they are allowed to register. Should you have any queries, please contact the Counter Fraud Unit.

25.5. With regard to shared services, the Council 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 DPs cannot make use of one Council's membership to obtain any information on behalf of another. Login details will be necessary for each Council that an individual is employed by or works on behalf of.

25.6. The online application form, once completed by the Applicant will be forwarded electronically to a SPoC at NAFN who will then perform their responsibilities and if required they will contact the Applicant regarding the contents of the application form. The SPoC at NAFN will obtain confirmation from the nominated DP that they are aware of the application before proceeding.

- 25.7. The SPoC confirms that the Council is permitted to use the recorded statutory purpose and determines the conduct to satisfy the Council's need (the type of data that is required). If event data is required the SPoC checks the Applicant has recorded a description of the offence(s) and a justification for the seriousness of the offence(s)
- 25.8. The SPoC can return the application to the Council for a re-work if it does not meet the necessary criteria.
- 25.9. Once approved the SPoC refers the application to OCDA for authorisation. OCDA then return the application to NAFN for the SPoC to obtain the authorised data from the CSP.
- 25.10. If the OCDA officer rejects the application it can be returned to the applicant for a re-work.

26. TIME SCALES

- 26.1. A new Operational Prioritisation has been introduced to enable NAFN to convey to OCDA the operational urgency for the acquisition of data and ensure it is appropriately triaged and handled to meet these demands.
- 26.2. Operational Prioritisation is categorised in Priority Levels 1-4 and for each Priority rating there is an expected Service response time.
- 26.3. The Council will generally be submitting requests that are Priority Level 4 – Routine- for which the response should be within 4 working days or 60 working hours.

27. APPLICATION FORM

- 27.1. The Applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for CD.
An application to acquire CD must:
- describe the CD required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
 - specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
 - include a unique reference number;
 - include the name and the office, rank or position held by the person making the application;
 - describe whether the CD relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
 - identify and explain the time scale within which the data is required;
 - explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
 - present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;

- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data
- include the operation name (if applicable) to which the application relates;

28. URGENT ORAL AUTHORISATION

- 28.1. There is no provision within the legislation for the Council to orally provide authority to obtain CD. All requests will be made in writing on the NAFN portal and require authorisation from a DP.

29. ERRORS

- 29.1. There is a requirement to record or in some instances report to IPCO errors that occur when accessing CD. The thorough checking of operating procedures, including the careful preparation and checking of applications, Notices and Authorisations, should reduce the scope for making errors. Attention to detail will be required by all persons involved in the process.
- 29.2. Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of CD that require further improvement to eliminate errors and the risk of undue interference with any individual's rights. Therefore, the SPoC or other persons involved in the process should bring to the immediate attention of the SRO either a recordable error or a reportable error and the necessary action can then be taken in line with the COP.
- 29.3. Where material is disclosed by a CSP in error, which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, that material and any copy of it should be destroyed as soon as the report to the Commissioner has been made.
- 29.4. An error can only occur after:
- The granting of an Authorisation and the acquisition of data has been initiated, or
 - Notice has been given and the Notice has been served on a CSP in writing, electronically or orally.
- 29.5. It is important to apply the procedures correctly to reduce the risk of an error occurring. Where any error occurs, a record will be kept.
- 29.6. There are two types of errors:
- Reportable
 - Recordable

30. REPORTABLE ERROR

- 30.1. Where CD is acquired or disclosed wrongly a report must be made to the IPCO. Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error.
- 30.2. Examples can include:
- An Authorisation or Notice made for a purpose, or for a type of data which the relevant public authority cannot call upon or seek, under the Act;
 - Human error, such as incorrect transposition of information from an application to an Authorisation or Notice;
 - Disclosure of the wrong data by a CSP when complying with a Notice;
 - Acquisition of the wrong data by a public authority when engaging in conduct specified in an Authorisation;
- 30.3. Any reportable error must be reported to the SRO as soon as it is identified and then a report will be made to the IPCO 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 and indicate whether any unintended collateral intrusion has taken place. It will also provide 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.
- 30.4. If the report relates to an error made by a CSP, the Authority must still report it. The CSP should also be notified to enable them to investigate the cause.

31. RECORDABLE ERROR

- 31.1. In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the Council and NAFN of such occurrences. These records must be available for inspection by the IPCO.
- 31.2. The staff involved in the process of acquiring CD must report errors once they have been identified. It will not be acceptable for the error to be ignored.
- 31.3. Examples can include:
- A Notice given, which is impossible for a CSP to comply with and an attempt to impose the requirement has been undertaken by the public authority;
 - Failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation, or data for which the requirement to acquire or obtain it is known to be no longer valid.

32. EXCESS DATA

- 32.1. Where authorised conduct results in the acquisition of excess data, the excess data acquired or disclosed should only be retained by the public authority where appropriate to do so – for example in relation to a criminal investigation.
- 32.2. Where a public authority is bound by the Criminal Procedure and Investigations Act 1996 and the IPA Codes of Practice, there will be a requirement to record and retain

data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid authorisation.

- 32.3. If having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The SRO (or a person of equivalent grade or authority) will review the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation.
- 32.4. As with all CD, the requirements of relevant data protection legislation and data retention policies should be adhered to in relation to excess data.

33. RECORD KEEPING AND SECURITY OF DATA

- 33.1. All the records and any data obtained must be kept secure and confidential.
- 33.2. The Council must retain copies of all Applications, as a printed copy of the online application submitted via NAFN, and any other associated documentation where copies have been provided by the NAFN SPoC. This will be coordinated by the RIPA Coordinating Officer/DP who also holds copies of applications for surveillance as per the Council's overarching RIPA Policy.
- 33.3. The copy application records must be available for inspection by the IPCO. The IPCO will also be able to obtain copies direct from NAFN.
- 33.4. The SRO will have access to all of these forms as and when required.
- 33.5. The Council 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;
 - The reason for any referrals back or rejections;
 - 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);

34. CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996 (CPIA)

- 34.1. The Criminal Procedure and Investigations Act 1996 (CPIA) requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor. Therefore, all material relating to the accessing of CD falls under these provisions. If the Applicant is not the Disclosure Officer in the case, they must make the Disclosure Officer aware of all of the material relating to the application and acquisition of the CD.
- 34.2. All material which may be relevant to the investigation must be retained until a decision is taken whether to institute proceedings against a person for an offence and if prosecuted, at least until the accused is acquitted or convicted, or the prosecutor decides not to proceed with the case and in line with the Council's Data Retention Policies.

34.3. Where the accused is convicted, the data which is relevant must be retained at least for six months from the date of conviction, and where the court imposes a custodial sentence, until the convicted person is released from custody.

34.4. If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction and in line with the Council's Data Retention Policies.

35. DATA PROTECTION ACT 2018 (DPA) AND THE GENERAL DATA PROTECTION REGULATIONS (GDPR)

35.1. CD acquired or obtained under the provisions of the IPA, and all copies, extracts and summaries of it must be handled and stored securely in line with the requirements of data protection legislation and regulations.

35.2. There is no provision in the IPA preventing CSPs from informing individuals about the disclosure of their CD in response to a Subject Access Request. However, a CSP may exercise certain exemptions to the right of subject access. If a CSP receives a Subject Access Request they must carefully consider whether in the particular case, disclosure of the fact of the Notice would be likely to prejudice the prevention or detection of crime.

35.3. Should a request for advice be made from a CSP to the SPoC regarding a disclosure, the SPoC will consult with the Data Protection Officer for the Council and the Applicant if necessary before a decision is made. Each case should be examined on its own merits.

35.4. Equally, these rules will apply should a Subject Access Request be made from an individual where material under this legislation is held by the Council.

35.5. A record will be made of the steps taken in determining whether disclosure of the material would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner and the courts etc.

36. OVERSIGHT

36.1. The IPA provides for an Investigatory Powers Commissioner (IPC) whose remit includes providing comprehensive oversight of the use of the powers contained within the IPA and adherence to the practices and processes in the Code of Practice. They carry out inspections, and for the purposes of Council applications, carry out inspections of NAFN. Should they have any concerns regarding an application they would contact the relevant staff involved at the Council. It is possible that they could also inspect the Council.

36.2. It is important to note that should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the IPA in relation to the acquisition or disclosure of CD, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal.

37. COMPLAINTS

37.1. The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with the Act. Any concerns about compliance with data protection and related legislation should be passed to the ICO at the following address:

37.2. Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
0303 123 1113
www.ico.org.uk

The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers, including those covered by the IPA.

The IPT is an independent body made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint the IPT can undertake its own enquiries and complaints and can demand access to all information necessary. Information regarding the IPT and how to make a complaint can be found at www.ipt-uk.com, or by writing to:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

38. STRATEGY AND POLICY REVIEW

38.1. The Counter Fraud Unit 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.

Responsible Department: Counter Fraud Unit

Date: April 2019

Review frequency as required by legislative changes / every year.

This page is intentionally left blank

Audit Committee 2019-20 work plan

| Item | Author |
|------|--------|
|------|--------|

| 22 January 2020 (Report deadline: 10 January 2020) | |
|---|--------------------|
| Cyber Security update | IT |
| Audit committee update (including audit cope and additional work letter) | Grant Thornton |
| Internal audit monitoring report | Internal Audit |
| Revised RIPA (surveillance and CHIS) Policy and PA (communications data) Policy | Counter Fraud Unit |
| 24 March 2020 (Report deadline: 12 March 2020) | |
| Audit committee update | Grant Thornton |
| Audit plan (for the current year) | Grant Thornton |
| Certification of grants and returns (for the previous year) | Grant Thornton |
| Annual plan (for the upcoming year) | Internal Audit |
| Internal audit monitoring report | Internal Audit |
| Counter Fraud update and future work provision | Counter Fraud Unit |
| Annual review and approval of RIPA guidance policies | Counter Fraud Unit |
| Annual review of Code of Corporate Governance | Darren Knight |
| Annual Governance Statement | Darren Knight |
| Annual Review of Risk Management Policy | Ann Wolstencroft |
| 22 July 2020 (Report deadline: 10 July 2020) | |
| Internal audit opinion (for the previous year) | Internal Audit |
| Annual Audit Fee letter for the coming year | Grant Thornton |
| Audit highlights memorandum - ISA 260 (for the previous year) inc. Financial Resilience | Grant Thornton |
| Auditing Standards – communicating with the Audit Committee | Paul Jones |
| Statement of Accounts (previous year) (inc. letter of representation) | Finance Team |

| ANNUAL ITEMS (standing items to be added to the work plan each year) | |
|--|----------------|
| January | |
| IT Security update | IT |
| Audit committee update | Grant Thornton |
| Certification of grants and returns (for the previous year) | Grant Thornton |
| Internal audit monitoring report | Internal Audit |

Audit Committee 2019-20 work plan

| Item | Author |
|---|--------------------|
| Annual governance statement – significant issues action plan | Internal Audit |
| April | |
| Audit committee update | Grant Thornton |
| Audit plan (for the current year) | Grant Thornton |
| Annual plan (for the upcoming year) | Internal Audit |
| Internal audit monitoring report | Internal Audit |
| Counter Fraud update and future work provision | Counter Fraud Unit |
| Annual review and approval of RIPA guidance policies | Counter Fraud Unit |
| Annual review of Code of Corporate Governance | Darren Knight |
| Annual Governance Statement | Darren Knight |
| Annual Review of Risk Management Policy | Ann Wolstencroft |
| July | |
| Internal audit opinion (for the previous year) | Internal Audit |
| Annual Audit Fee letter for the coming year | Grant Thornton |
| Audit highlights memorandum - ISA 260 (for the previous year) inc. Financial Resilience | Grant Thornton |
| Auditing Standards – communicating with the Audit Committee | Paul Jones/Chair |
| Statement of Accounts (previous year) (inc. letter of representation) | Finance Team |
| September | |
| Internal audit monitoring report | Internal Audit |
| Counter Fraud update and future work provision | Counter Fraud Unit |
| Annual audit letter (for the previous year) | Grant Thornton |