Cheltenham Borough Council

Audit Committee – 23 March 2016

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

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

Investigatory Powers Act 2000 (RIPA) (appendix 3)

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

1. Background - Existing policy review

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

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

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

2. RIPA Authorisations

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

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

3. Revised RIPA Policy Guidelines

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

Internet Investigations

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

Reporting errors

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

Surveillance outside of RIPA

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

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

Equipment

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

Joint Agency Surveillance

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

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

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

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

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

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

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

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

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

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

Communications data available to local authorities

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

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

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

Services:

The Council is not allowed to access:

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

Power to obtain communications data

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

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

4.13 2. An authorisation under S22(3).

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

Procedure for Obtaining Communications Data

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

Roles and responsibilities

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

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

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

Central Records

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

Interception of Communications Commissioner's Office

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

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

Strategy and Policy Review

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

5. Reasons for recommendations

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

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

6. Alternative options considered

6.1 None

7. Consultation and feedback

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

8. Performance management – monitoring and review

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

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

Risk Assessment **Appendix 1**

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

	Councils reputation and assets are put at risk.										

Explanatory notes

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

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

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

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