Cheltenham Borough Council

Cabinet – 6 December 2016

Acquisition of Communications Data using The Regulation of Investigatory Powers Act 2000 (RIPA) Policy

Accountable member	Cabinet Member Corporate Services, Councillor Roger Whyborn
Accountable officer	Pat Pratley, Head of Paid Service
Ward(s) affected	**All**
Key/Significant Decision	**No**
Executive summary	A new Policy and Procedures Document for the Acquisition of Communications Data using The Regulation of Investigatory Powers Act 2000 (RIPA) has been drafted by the Counter Fraud Unit to provide transparency and guidance on the process. A Local Authority must be a paid up member of the 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. The policy details how RIPA controls the process by which the Council obtains communications data. 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. The draft Policy has been developed in consultation with other Gloucestershire authorities and West Oxfordshire District Council to provide continuity for the operation of the Counter Fraud Unit and shared Enforcement Officers. The draft policy was considered by Cheltenham Borough Council's Audit Committee on the 23 March 2016.
Recommendations	**That Cabinet:** **1. Consider and approve the new Policy and Procedures Document for the Acquisition of Communications Data using The Regulation of Investigatory Powers Act 2000 (RIPA).** **2. Authorise the Counter Fraud Unit to make any future amendments to the policy to reflect legislative changes, in consultation with appropriate Officers, including the Cabinet Member and Leader of the Council, and with One Legal.**

Financial implications	There are no direct financial implications as a result of this report. However, the adoption of this policy will help to support the prevention and detection of misuse of public funds and fraud therefore reducing potential financial loss to the council. **Contact officer: Paul Jones, S151 Officer, Cheltenham BC** **Paul.Jones@cheltenham.gov.uk**
Legal implications	This report ensures that the Council complies with the legislation and guidance issued by the Home Office. The Council may where it is necessary and proportionate need to apply for communications data to assist with an investigation. 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 RIPA Policies 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 the use of surveillance and communication data access Judicial approval will be required before an Authorisation is granted **Contact officer: Donna Marks, One Legal** **donna.marks@tewkesbury.gov.uk 01684 272068**
HR implications (including learning and organisational development)	All Council employees who are employed within an enforcement role will need to be made aware of the policy. Regular training sessions will be provided to ensure that staff are fully conversant with The Regulation of Investigatory Powers Act 2000. **Contact officer: Julie McCarthy, HR Manager (West)** **Julie.McCarthy@cheltenham.gov.uk**
Key risks	If the Council obtains communications data without due regard to RIPA, Ministry of Justice Codes of Practice and the CBC policy and procedural guidance then there are risks to an individual's rights, including any breach of Human Rights – right to privacy, and to the Council's reputation.
Corporate and community plan Implications	In administering its responsibilities; this Council has a duty to prevent fraud and corruption, whether it is attempted by someone outside or within the Council such as another organisation, a resident, an employee or Councillor. The Council is committed to an effective counter fraud and corruption culture, by promoting high ethical standards and encouraging the prevention and detection of fraudulent activities using robust enforcement techniques, thus supporting corporate and community plans.
Environmental and climate change implications	None directly arising from the report.

Property/Asset Implications	None directly arising from the report. **Contact officer: David Roberts, Head of Property Services** **david.roberts@cheltenham.gov.uk**

1. Background

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

1.2. This policy is an additional one which relates to the acquisition of communications data for intelligence purposes by the Council.

1.3. Since September 2014, Local Authorities can only access communications data via the National Anti-Fraud Network (NAFN). 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.

1.4. This procedural guide is based on the requirements of The Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office Code of Practice on the Acquisition and Disclosure of Communications Data. If any of the Home Office Codes of Practice change, the appropriate guide will be updated, and the amended version placed on the internet / published accordingly. Regular training sessions will also be provided to ensure that staff members are fully conversant with the Act.

1.5. Part 1 Chapter 2 of RIPA controls the obtaining of communications data by Local Authority staff. This data does not include the content of the communications i.e. the actual email, message, letter, text or telephone conversation. Part 1 also introduces a statutory framework to regulate access to communications data by public bodies consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in these processes. In addition it puts safeguards in place to balance the rights of the individual against the needs of society, as a whole, to be protected from crime and other public safety risks. This thus reflects the requirements of Article 8 of the European Convention on Human Rights; the right to privacy.

1.6. 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.

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

(i) Subscriber Information (RIPA S21(4)(c)) - Information about Communications Services Users:
(ii) Service Use Data (RIPA S 22(4)(b) - Information about the use of Communications Services:

1.8. The Council is not allowed to access traffic data as detailed within section 3.2 of the policy.

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

1.10. Procedure for Obtaining Communications Data: 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 Counter Fraud Unit.

1.11. Roles and Responsibilities: The policy provides for the roles and responsibilities of those involved in the process. The Senior Responsible Officer (the Head of Paid Service) 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.

1.12. Strategy and Policy Review: 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.

2. Reasons for Recommendations

2.1. 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.

2.2. If authorisation is given for communications data to be obtained, a central record will be maintained and a report will be provided to Audit Committee.

3. Consultation

3.1. The Corporate Governance Group, the Counter Fraud Unit and officers involved in investigation and surveillance activities work have been consulted. Advice has also been sought from One Legal.

3.2. The Audit Committee considered the draft policy in March 2016. The Audit Committee made no changes to the document and unanimously endorsed it.

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

Report author	**Emma Cathcart, Counter Fraud Team Leader** **Emma.Cathcart@cotswold.gov.uk** **01285 623356**
Appendices	1. Risk assessment 2. Acquisition of Communications Data (RIPA) 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	Likeli-hood 1-6	Score	Control	Action	Deadline	Responsible officer	Transferred to risk register
1	If the Council fails to put in place adequate policy and procedures in relation to the application of RIPA when obtaining communications data then there are risks to individuals rights and the Council's reputation.	Head of Paid Service	23.3.2016	4	2	8	Accept	Introduce a suitable policy and put in place effective management and guidance.	Ongoing	Counter Fraud Unit	
2	If the Council fails to promote intelligence gathering techniques such as acquiring communications data then the Council may not be able to robustly tackle the misuse of public funds	Head of Paid Service	14.11.2016	3	3	9	Accept	Promote awareness with Enforcement Officers throughout the Council.	Ongoing	Counter Fraud Unit	

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