COTSWOLD
DISTRICT COUNCIL

**AUDIT COMMITTEE** **24TH JANUARY 2017**

**AGENDA ITEM (13)**

**DRAFT REGULATION OF INVESTIGATORY POWERS ACT 2000 (COMMUNICATIONS DATA) POLICY**

| | |
|---|---|
| **Accountable Members** | Audit Committee |
| **Accountable Officer** | Jenny Poole<br>Group Manager GO Shared Services/Finance Lead 2020 Partnership<br>01285 623313<br>jenny.poole@cotswold.gov.uk |
| **Report Author** | Emma Cathcart<br>Counter Fraud Team Leader<br>01285 623356<br>emma.cathcart@cotswold.gov.uk |

| | |
|---|---|
| **Purpose of Report** | To present a draft Regulation of Investigatory Powers Act 2000 (Communications Data) Policy as part of the consultation process. |
| **Recommendation(s)** | **That the Audit Committee reviews the RIPA 2000 (Communications Data) Policy and forwards its comments thereon to the Cabinet.** |
| **Reason(s) for Recommendation(s)** | To ensure that an appropriate and robust Policy is in place.<br>The Audit Committee oversees the Council's counter fraud arrangements and it is therefore appropriate for the Committee to consider and comment on the attached Policy. |

| | |
|---|---|
| **Ward(s) Affected** | All |
| **Key Decision** | No |
| **Recommendation to Council** | No - the Committee's comments will be considered by Cabinet in February 2017. |

| | |
|---|---|
| **Financial Implications** | There are no direct financial implications as a result of this policy. 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. |

| | |
|---|---|
| **Legal and Human Rights Implications** | This report ensures that the Council complies with the legislation and guidance issued by the Home Office.<br><br>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.<br><br>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.<br><br>Judicial approval will be required before an Authorisation is granted. |
| **Environmental and Sustainability Implications** | None directly arising from the report. |
| **Human Resource Implications** | None directly arising from the report. |
| **Key Risks** | The Council is required to proactively tackle fraudulent activity in relation to the abuse of public funds. The Counter Fraud Unit provides assurance in this area.<br>Failure to undertake such activity would accordingly not be compliant and expose the authority to greater risk of fraud and/or corruption.<br>It is essential that any application of the RIPA (Communications Data) Policy 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.<br>If the Council obtains communications data without due regard to RIPA, Ministry of Justice Codes of Practice and the Council's 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. |
| **Equalities Impact Assessment** | Not Required. |
| **Related Decisions** | None. |
| **Background Documents** | None. |
| **Appendices** | **Appendix 'A'** - Draft RIPA 2000 (Communications Data) Policy |
| **Performance Management Follow Up** | Regular updates are provided by the Counter Fraud Team Leader to Corporate Management Team and bi-annual reports in relation to counter fraud work will be submitted to the Audit Committee.<br><br>Policy documentation will be presented when required. |
| **Options for Joint Working** | The attached draft policy is presented as part of the consultation process across all counter fraud partner Authorities across the region. |

**Background Information**

1. 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 copy of the Policy is attached at **Appendix 'A'**.

2. 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 policy 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.

3. 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 (such as 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.

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 interne/ published accordingly. Regular training sessions will also be provided to ensure that staff members are fully conversant with the provisions of the Act.

5. 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 e-mail message, letter, text or telephone conversation merely details basic subscriber information and the frequency of communication). Section 3.1 of the policy details the type of information the Council is allowed to obtain - subscriber information and service use data. The Council is not allowed to access traffic data as detailed within section 3.2 of the policy.

6. A Local Authority may only acquire communications data for the purpose of the prevention or detection of crime or the prevention of disorder.

7. <u>Procedure for Obtaining Communications Data</u>

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 applicants' requests. Further information on this procedure is covered within section 5 of the policy and additional guidance can be provided by staff in the Counter Fraud Unit.

8. The draft Policy has been developed in consultation with other partner Councils to provide continuity for the operation of the Counter Fraud Unit and shared Enforcement Officers.

9. The Policy will be submitted to the Cabinet for consideration of approval, and the Audit Committee is asked to provide comments thereon to the Cabinet, to aid its deliberations.

(END)