



# COTSWOLD DISTRICT COUNCIL

Council name	<b>COTSWOLD DISTRICT COUNCIL</b>
Name and date of Committee	<b>CABINET – 2 DECEMBER 2019</b>
Report Number	<b>AGENDA ITEM 10</b>
Subject	<b>Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy</b> <b>Investigatory Powers Act 2016 Acquisition of Communications Data Policy</b>
Wards affected	All indirectly
Accountable member	Cllr Joe Harris, Leader of the Council Tel: 01285 623000 Email: <a href="mailto:Joe.Harris@cotswold.gov.uk">Joe.Harris@cotswold.gov.uk</a>
Accountable officer	Emma Cathcart, Counter Fraud Manager Tel: 01285 623356 Email: <a href="mailto:Emma.Cathcart@cotswold.gov.uk">Emma.Cathcart@cotswold.gov.uk</a>
Summary/Purpose	<p>To present Cabinet with:</p> <ul style="list-style-type: none"><li>i) A revised Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy for approval and adoption.</li><li>ii) A new Investigatory Powers Act 2016 Acquisition of Communications Data Policy for approval and adoption.</li></ul> <p>The Council 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 Council will abide by to mitigate the risk of legal challenge in Court.</p> <p>The Policy demonstrates the Council'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 Council's existing authorisation arrangements.</p>
Annexes	<a href="#">Annex A</a> – Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy <a href="#">Annex B</a> – Investigatory Powers Act 2016 Acquisition of Communications Data Policy

Recommendation/s	a) <i>Formally adopts the Policies attached to this report.</i> b) <i>Authorises the Group Manager Legal Services to approve future minor amendments to the Policies in consultation with the Counter Fraud Manager and the Leader of the Council.</i>
Corporate priorities	Ensure that all services delivered by the Council are delivered to the highest standard.
Key Decision	NO
Exempt	NO
Consultees/ Consultation	The Policies have been reviewed by the Legal Team and have been issued to Governance Group, Joint Management Team and Audit Committee for comment.

## 1. BACKGROUND

- 1.1. The Council'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 [Annex A](#) and at [Annex B](#), are revised Policies.
- 1.2. The Investigatory Powers Act 2016 now governs communication data requests. The legislation widened the scope of information the Council 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 Councils. 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 Council to nominate a Designated Senior Officer who will confirm to NAFN that the Council 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 Council must obtain judicial approval.
- 1.6. As outlined in 1.5 above, the Council 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 with staffing.

- 1.7. The Senior Responsible Officer is the Monitoring Officer, Bhavna Patel and the Authorising Officers are the Head of Paid Service, Nigel Adams and the Chief Finance Officer, Jenny Poole.
- 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. There were no RIPA applications made by the Council during 2018/2019. There was one Non-RIPA application made by the Counter Fraud Unit working with ERS.
- 1.10. Audit Committee endorsed the Policies on 14 November 2019.

## **2. FINANCIAL IMPLICATIONS**

- 2.1. The adoption and approval of these Policies will support the Council's objectives in reducing crime and financial loss to the Council.

## **3. LEGAL IMPLICATIONS**

- 3.1. The Council 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.
- 3.2. Any requests for directed/covert surveillance or the acquisition of communications data undertaken should be authorised by the appropriate Officer and recorded in the Central Register.
- 3.3. The Council 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.

## **4. RISK ASSESSMENT**

- 4.1. The Policies demonstrate the Council's consideration of necessity, proportionality and public interest when deciding on surveillance activity or the decision to obtain personal communication data.

## **5. EQUALITIES IMPACT**

- 5.1. 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 Council from allegations of the same.

## **6. BACKGROUND PAPERS**

- 6.1. The following documents have been identified by the author of the report in accordance with section 100D.5(a) of the Local Government Act 1972 and are listed in accordance with section 100 D.1(a) for inspection by members of the public:
  - Report to Cabinet dated 6 November 2014 and associated minutes.
  - Report to Cabinet dated 16 February 2017 and associated minutes.

**6.2.** These documents will be available for inspection at the Council Offices during normal office hours for a period of up to 4 years from the date of the meeting. Please contact the author of the report.