

TEWKESBURY BOROUGH COUNCIL

Report to:	Executive Committee
Date of Meeting:	18 November 2020
Subject:	Regulation of Investigatory Powers Act (RIPA) 2000 & Investigatory Powers Act (IPA) 2016
Report of:	Borough Solicitor
Corporate Lead:	Borough Solicitor
Lead Member:	Lead Member for Corporate Governance
Number of Appendices:	Two

Executive Summary:

To present Executive Committee with:

- i) A revised Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy.
- ii) A new Investigatory Powers Act 2016 Acquisition of Communications Data Policy.

The local authority is required to have effective policies to enable officers to gather intelligence and conduct surveillance in line with the law.

The policies set out the legislative framework and principles the Local Authority will abide by to mitigate the risk of legal challenge in Court.

The Policies demonstrate 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.

The Policies were endorsed by the Audit and Governance Committee in September 2020.

Recommendation:

- 1. That the Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy be APPROVED.**
- 2. That the Investigatory Powers Act 2016 Acquisition of Communications Data Policy be APPROVED.**
- 3. That approval of future minor amendments be delegated to the Borough Solicitor, in consultation with the Counter Fraud Unit Manager and the Lead Member for Corporate Governance.**

Reasons for Recommendation:

To update and replace the existing RIPA Procedural Guide in line with changes to the legislation.

Effective enforcement plays an important role in enabling the local authority to achieve its priorities and community outcomes.

Resource Implications:

The adoption and approval of these policies will support the local authority's objectives in reducing crime and financial loss to the local authority.

Legal Implications:

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.

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.

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.

Risk Management Implications:

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.

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.

Performance Management Follow-up:

None directly arising from this report.

Environmental Implications:

None directly arising from this report.

1.0 INTRODUCTION/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 1 and at Appendix 2 are revised policies. These policies have been reviewed by the Investigatory Powers Commissioner's Office Inspector and the suggested minor amendments have been incorporated.

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 will be 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 The local authority must have a Senior Responsible Officer and Authorising Officers to approve the application before the Court is approached. The Borough Solicitor is the Senior Responsible Officer and the Authorising Officers are the Head of Finance and Asset Management and the Head of Community Services.
- 1.7 The role of RIPA Coordinator has been transferred to the Counter Fraud Unit Manager who will be responsible for the management of policies, annual updates to Members, the return of statistics to the Investigatory Powers Commissioners Office, coordination of any inspections by the Investigatory Powers Commissioners Office and the management and recording of all applications by Officers of the local authority.
- 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 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.

2.0 UPDATED POLICY

- 2.1 These two policies replace The RIPA Procedural Guide.
- 2.2 The Social Media Policy is currently undergoing a review and will be the subject of consultation with the Corporate Governance Group and Management Team prior to approval by Members.

3.0 OTHER OPTIONS CONSIDERED

- 3.1 None.

4.0 CONSULTATION

- 4.1 The draft policies were subject to consultation with the Corporate Governance Group, Management Team and One Legal.

5.0 RELEVANT COUNCIL POLICIES/STRATEGIES

- 5.1 None.

6.0 RELEVANT GOVERNMENT POLICIES

6.1 Home Office Codes of Practice.

7.0 RESOURCE IMPLICATIONS (Human/Property)

7.1 Council staff with responsibility for enforcement and Authorising Officers will be made aware of the updated policies and receive training.

8.0 SUSTAINABILITY IMPLICATIONS (Social/Community Safety/Cultural/ Economic/ Environment)

8.1 None.

9.0 IMPACT UPON (Value For Money/Equalities/E-Government/Human Rights/Health And Safety)

9.1 The legislation 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.

10.0 RELATED DECISIONS AND ANY OTHER RELEVANT FACTS

10.1 Audit and Governance Committee – 23 September 2020.

Background Papers:

None.

Contact Officer:

Counter Fraud Manager Tel: 01285 623356
Email: emma.cathcart@cotswold.gov.uk

Appendices:

1 – Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy.
2 - Investigatory Powers Act 2016 Acquisition of Communications Data Policy.