# TEWKESBURY BOROUGH COUNCIL

| | |
|---|---|
| **Report to:** | Audit and Governance Committee |
| **Date of Meeting:** | 21 July 2021 |
| **Subject:** | Use of the Internet and Social Media in Investigations and Enforcement Policy |
| **Report of:** | Counter Fraud Unit Manager |
| **Corporate Lead:** | Head of Finance and Asset Management |
| **Lead Member:** | Lead Member for Corporate Governance |
| **Number of Appendices:** | 1 |

**Executive Summary:**

To provide the Audit and Governance Committee with an updated and revised Use of the Internet and Social Media in Investigations and Enforcement Policy.

**Recommendation:**

**To RECOMMEND TO THE EXECUTIVE COMMITTEE that:**

1. **The Use of the Internet and Social Media in Investigations and Enforcement Policy, as attached at Appendix 1, be APPROVED.**
2. **That authority be delegated to the Borough Solicitor, in consultation with the Counter Fraud Unit Manager and the Lead Member for Corporate Governance, to approve future minor amendments to the policy.**

**Reasons for Recommendation:**

To introduce an updated Use of the Internet and Social Media in Investigations and Enforcement Policy to reflect the Investigatory Powers Commissioner's Office (IPCO) guidance and recommendations as outlined within the recent Inspection Report.

**Resource Implications:**

The adoption and approval of this Policy will support the Council's objectives in reducing crime and financial loss.

**Legal Implications:**

The Council is required to ensure that it complies with the Regulation of Investigatory Powers Act 2000 (RIPA) , the Investigatory Powers Act 2016 (IPO) and any other relevant/statutory legislation regarding investigations. Any authorisations for directed/covert surveillance or the acquisition of communications data undertaken should be authorised by the appropriate Officer and recorded in the Central Register.

**Risk Management Implications:**

The RIPA and IPA 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. The application of the policies and procedures, to govern surveillance and the obtaining of personal communications data, minimises the risk that an individual's human rights will be breached. Furthermore, it protects the Council from allegations of the same.

**Performance Management Follow-up:**

Not applicable

**Environmental Implications:**

Not applicable

## 1.0 INTRODUCTION/BACKGROUND

**1.1** The Counter Fraud Unit was tasked with reviewing and developing the Council's policy and procedures on accessing the internet and social media for investigations and enforcement purposes.

## 2.0 USE OF THE INTERNET AND SOCIAL MEDIA IN INVESTIGATIONS AND ENFORCEMENT POLICY

**2.1** Whilst there has been a general decline in the use of covert surveillance activity, Councils have come under increased scrutiny in this area by Investigatory Powers Commissioner's Office (IPCO) during inspections and there are a number of recommendations in their annual reports, procedures and guidance.

**2.2** IPCO confirms that, where inspections reveal activity - particularly with regard to intelligence gathering through the use of the internet and social media - evidence should demonstrate that consideration has been given to whether the activity could be considered surveillance and the appropriate authorisation sought.

**2.3** Existing arrangements have been reviewed and the policy for ensuring compliance has been developed, attached at Appendix 1. The policy is generic and broad to ensure that the integrity of investigations and methods of detection are not revealed.

**2.4** The procedure that derives from this policy is a confidential document available to members of staff involved in investigation work only who are authorised to undertake research and investigation using open source internet applications (as investigative tools) or other civil or criminal enforcement and recovery work.

## 3.0 OTHER OPTIONS CONSIDERED

**3.1** None

## 4.0 CONSULTATION

**4.1** The Policy was subject to consultation with Operational Managers, the Corporate Governance Group, Management Team and One Legal.

**5.0 RELEVANT COUNCIL POLICIES/STRATEGIES**

**5.1** Regulation of Investigatory Powers Act 2000 (Surveillance and CHIS) Policy

**6.0 RELEVANT GOVERNMENT POLICIES**

**6.1** None

**7.0 RESOURCE IMPLICATIONS (Human/Property)**

**7.1** Council staff with enforcement responsibilities will be made aware of the policy.

**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 application of the RIPA and IPA 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.

**10.0 RELATED DECISIONS AND ANY OTHER RELEVANT FACTS**

**10.1** None

---

**Background Papers**: Report to Executive Committee, November 2020

**Contact Officer:** Counter Fraud Unit Manager
01285 623356 emma.cathcart@cotswold.gov.uk

**Appendices:** Appendix 1 – Use of the Internet and Social Media in Investigations and Enforcement Policy