



WEST OXFORDSHIRE
DISTRICT COUNCIL

WEST OXFORDSHIRE DISTRICT COUNCIL

Name and date of Committee	Cabinet Wednesday 10 November 2021
Report Number	Agenda Item No. 8
Subject	Use of the Internet and Social Media in Investigations and Enforcement Policy
Wards affected	All indirectly
Accountable member	Councillor Michele Mead, Leader of the Council Email: Michele.Mead@westoxon.gov.uk
Accountable officer	Emma Cathcart, Counter Fraud Unit Manager Email: Emma.Cathcart@cotswold.gov.uk
Summary/Purpose	To present Cabinet with a new Use of the Internet and Social Media in Investigations and Enforcement Policy for adoption.
Annexes	Annex A – Use of the Internet and Social Media in Investigations and Enforcement Policy
Recommendation	(a) That Cabinet approves and adopts the Policy attached to this report; and (b) That Cabinet authorise the Chief Executive to approve future minor amendments to the Policy in consultation with the Counter Fraud Unit Manager, Legal Services and the Leader of the Council.
Corporate priorities	In administering its responsibilities the Council has a duty to enforce the law and prevent wrongdoing, whether it is attempted by someone outside or within the Council such as another organisation, a resident, an employee or a Councillor, thus supporting corporate priorities and community plans.
Key Decision	No
Exempt	No
Consultees/ Consultation	Any Policies drafted or revised by the Counter Fraud Unit have been reviewed by Legal Services and have been issued to the Governance Group, Corporate Management and Audit and General Purposes Committee for comment.

1. 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. MAIN POINTS

- 2.1. The Council's Policies are based on the legislative requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) and the Codes of Practice relating to directed surveillance and the acquisition of communications data.
- 2.2. 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.
- 2.3. 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.
- 2.4. Existing arrangements have been reviewed and the Policy for ensuring compliance has been developed, attached at Appendix A. The Policy is generic and broad to ensure that the integrity of investigations and methods of detection are not revealed.
- 2.5. 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.
- 2.6. The Council takes responsibility for ensuring its procedures relating to surveillance and the acquisition of communications data are continuously improved and all activity is recorded.
- 2.7. Audit and General Purposes Committee endorsed the Policy on 23 September 2021.

3. FINANCIAL IMPLICATIONS

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

4. LEGAL IMPLICATIONS

- 4.1. 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 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.

- 4.2. 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 Policies.

5. RISK ASSESSMENT

- 5.1. 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.

6. EQUALITIES IMPACT

- 6.1. The application of the RIPA and IPA 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.

7. ALTERNATIVE OPTIONS

- 7.1. None.

8. BACKGROUND PAPERS

- 8.1. Cabinet Report December 2019 - Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy / Investigatory Powers Act 2016 Acquisition of Communications Data Policy.