Cheltenham Borough Council

Audit, Compliance and Governance Committee – 22 September 2021

Use of the Internet and Social Media in Investigations and Enforcement Policy

Accountable Member	Leader of the Council, Councillor Rowena Hay
Accountable Officer	Paul Jones Executive Director Finance and Assets Paul.Jones@cheltenham.gov.uk
Ward(s) affected	All indirectly
Key/Significant Decision	No
Executive summary	To present the Audit, Compliance and Governance Committee with a new Use of the Internet and Social Media in Investigations and Enforcement Policy for comment.
Recommendations	**That the Audit, Compliance and Governance Committee considers the Use of the Internet and Social Media in Investigations and Enforcement Policy and provides comment to Cabinet.**
Financial implications	The adoption and approval of this Policy will support the Council's objectives in reducing crime and financial loss. **Contact Officer: Paul Jones, Executive Director Finance and Assets** Paul.Jones@cheltenham.gov.uk
Legal implications	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 as well as current Data Protection legislation. Any authorisations for directed/covert surveillance or the acquisition of communications data undertaken should be recorded appropriately in the Central Register. 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. The adoption of the policy is, under the Policy Framework, a matter for Cabinet. **Contact officer: One Legal** Legalservices@tewkesbury.gov.uk
HR implications (including learning and organisational development)	Council staff with enforcement responsibilities will be made aware of this Policy. **Contact officer: Clare Jones, , HR Business Partner** Clare.Jones @publicagroup.uk 01242 264355
Key risks	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.
Corporate and community plan Implications	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 Councillor, thus supporting corporate priorities and community plans.
Environmental and climate change implications	N/A
Property/Asset Implications	There are no property implications associated with this report. **Contact officer: Gemma Bell, Head of Finance and Property** Gemma.Bell@cheltenham.gov.uk

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.

1.2. 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.

1.3. 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.

1.4. 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.

1.5. Existing arrangements have been reviewed and the Policy for ensuring compliance has been developed, attached at Appendix 2. The Policy is generic and broad to ensure that the integrity of investigations and methods of detection are not revealed.

1.6. 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.

1.7. 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.

Report author	Emma Cathcart Counter Fraud Unit Manager 01285 623356 Emma.Cathcart@cotswold.gov.uk
Appendices	1. Risk Assessment 2. Use of the Internet and Social Media in Investigations and Enforcement Policy
Background Information	Cabinet Report – February 2020 Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy / Investigatory Powers Act 2016 Acquisition of Communications Data Policy

Risk Assessment

Appendix 1

The risk				Original risk score (impact x likelihood)			Managing risk				
Risk ref.	**Risk description**	**Risk Owner**	**Date raised**	**Impact 1-5**	**Likeli-hood 1-6**	**Score**	**Control**	**Action**	**Deadline**	**Responsible officer**	**Transferred to risk register**
1	If the Local Authority fails to put in place adequate policy and process covering the use of RIPA / IPA powers then it risks damage to its reputation and financial loss	Chief Executive	January 2020	4	2	8		Put in place effective management and guidance. Promote the guidance with mangers and enforcement officers	Ongoing	Chief Executive	

Explanatory notes

Impact – an assessment of the impact if the risk occurs on a scale of 1-5 (1 being least impact and 5 being major or critical)

Likelihood – how likely is it that the risk will occur on a scale of 1-6

(1 being almost impossible, 2 is very low, 3 is low, 4 significant, 5 high and 6 a very high probability)

Control - Either: Reduce / Accept / Transfer to 3rd party / Close