Version Control	
Document Name:	Use of the Internet and Social Media for Investigations and Enforcement Policy
Version:	1
Responsible Officer:	Emma Cathcart, Counter Fraud and Enforcement Unit
Approved by:	Cabinet / Executive / Audit & Standards Committee
Next Review Date	May 2023
Retention Period:	N/A

Revision History

Revision date	Version	Description

Consultees

Internal	External
Enforcement Lead Officers Governance Groups One Legal / Legal Services Corporate / Executive / Senior Leadership Audit / Audit and Governance / Audit, Compliance and Governance Committee	

Distribution

Name	
Enforcement Officers	

CONTENTS

1. INTRODUCTION

1.1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise, to use as intelligence and evidence.

1.2 The use of online open source Internet and Social Media research is a method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues. However, the use of the Internet and Social Media is constantly evolving and with it the risks, particularly regarding breaches of privacy under Article 8 of the Human Rights Act (HRA) 1998 and other operational risks.

1.3 The Council is a Public Authority in law under the HRA, and as such, the staff of the Authority must always work within this legislation. This applies to research on the Internet.

1.4 Researching, recording, storing, and using open source information regarding a person or group of people must be both necessary and proportionate and take account of the level of intrusion against any person. The activity may also require authorisation and approval by a Magistrate under the Regulation of Investigatory Powers Act (RIPA) 2000. To ensure that any resultant interference with a person's Article 8 Right (respect for private and family life) is lawful, the material must be retained and processed in accordance with the principles of the General Data Protection Regulation (GDPR) 2016 and Data Protection legislation.

2. SCOPE OF POLICY

2.1 This Policy and associated Procedure establishes the Council's approach to ensuring that all online research and investigations are conducted lawfully and ethically to reduce risk. It provides guidance to all staff within the Council, about legislative framework and implications associated with online Internet and Social Media research, when engaged in their official capacity. It will also ensure that the activity undertaken, and any evidence obtained, will withstand scrutiny.

2.2 This Policy takes account of the HRA, RIPA, Criminal Procedures and Investigations Act (CPIA) 1996, Data Protection legislation and regulations and National Police Chiefs Council (NPCC) Guidance on Open Source Investigation/Research.

2.3 This Policy and associated Procedure will be followed at all times and should be read, where required, with the RIPA Codes of Practice and any other legislation

and relevant policies mentioned in this document. Should there be any queries advice can be sought from the RIPA Coordinator within the Counter Fraud Unit.

2.4 This Policy should not be exempt from disclosure under the Freedom of Information Act 2000.

3. RISK

3.1 Staff must be aware that any activity carried out using the Internet leaves a trace or footprint which can identify the device used, and, in some circumstances, the individual carrying out the activity. This may pose a legal and reputational risk to the Council if they are challenged by the subject of the research for breaching Article 8.1 of the HRA which states "Everyone has the right to respect for his private and family life, his home and his correspondence".

3.2 Article 8.2 states "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others". It is therefore important that the Council can demonstrate that such activity was necessary and proportionate.

3.3 Monitoring of an individual's social media or other open source information on a repeated or continuous basis could constitute surveillance by a Public Authority and fall with the realms of RIPA.

3.4 Breach of an individual's rights under the HRA leaves the Council open to claims for financial compensation and the consequential reputational damage.

3.5 Failure to implement and follow a policy could risk compromising the integrity of evidence and any associated investigation.

4. NECESSITY / JUSTIFICATION

4.1 To justify the intrusion and interference with an individual's privacy there must be a clear and lawful reason for the activity. Therefore the necessity for the research such as the criminal conduct that it is aimed to prevent or detect must be identified and clearly described. This should be documented with clear objectives. Should the research fall within RIPA activity, the RIPA authorisation will deal with the criteria for it to be lawful intrusion.

5. PROPORTIONALITY

5.1 Proportionality involves balancing the level of intrusion of the research on the subject and other innocent third parties who might be affected by it (collateral intrusion) against the need for the activity in operational terms.

5.2 The Officer must consider and document the benefit to carrying out the activity and how the benefit will outweigh the intrusion.

5.3 The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

5.4 All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

6. PRIVATE INFORMATION

6.1 Private information is defined in the RIPA Codes of Practice and states it "includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships."

6.2 Prior to, and during, any research Staff must take into account the privacy issues of any person associated with the research.

6.3 There are three broad categories of private information applicable here:

6.4 Category 1 - Viewing publically available postings or websites where the person viewing does not have to register a profile, answer a question, or enter any significant correspondence in order to view. For example, a typical trader's website.

6.5 Category 2 - Viewing postings on social networks where the viewer has had to register a profile but otherwise there is no other restriction on access. This would include Facebook where there is no need to be accepted as a "friend" to view. For example a trader has a "shop window" on Facebook advertising a business and products.

6.6. Category 3 - Viewing postings on social networks which require a "friend" or similar status to view.

7. REVIEWING THE ACTIVITY

7.1 During the course of conducting the Internet open source research, the nature of the online activity may evolve. It is important that Staff continually assess and review their activity to ensure it remains lawful and compliant. Where it evolves into RIPA activity, the RIPA procedure should be followed. If in doubt, Staff should seek advice from the RIPA Coordinator within the Counter Fraud Unit.

8. USE OF MATERIAL

8.1 The material obtained from conducting open source Internet and Social Media research may be used as intelligence or evidence.

8.2 Any material gathered from the Internet during the course of a criminal investigation must be retained in compliance with the Criminal Procedure and Investigations Act (CPIA) Codes of Practice and all material stored in line with the General Data Protection Regulations (GDPR) data retention policies.