Online Investigations Policy

(Use of online material for enquiries/investigations)

MARCH 2023

Version Control			
To be reviewed every two years			
Date	**Version No**	**Reason for Change**	**By whom**
September 2019	V1	New policy following inspection by OSC in May 2016	Trading Standards & Community Protection Manager Acting Audit Manager
March 2023	V2	Review to align with guidance contained in the Covert Surveillance and Property Interference Code of Practice (2018) following inspection by IPCO in November 2022	Information Rights Manager (DPO) Trading Standards & Community Protection Manager

1 Introduction

1.1 The increase in the use of the internet by residents and businesses in Cheshire East is evident. The advent of social media sites has also created the ability for individuals, businesses and organisations to easily communicate between each other, serving as a useful tool to keep in touchand interact on what can be a real time basis.

1.2 People or groups can instantaneously share information, coordinate eventsand provide updates that are of interest to their friends, family, or customer base.

1.3 Social media sites can also serve as a platform for individuals or groups to express their opinions and social, political and religious beliefs to give just a few common examples.

1.4 It is also possible to share photographs or videos with others and indeedwhere privacy settings allow, to share the posts of other people not necessarily connected with the original person.

1.5 A wealth of data is available via the internet to members of the public as well as officers of the Council. Online research and investigation has therefore become an extremely useful tool for officers and investigators to prevent, detect and investigate:

- suspected criminal activity
- harm to residents and businesses and ensuring safeguarding measures are in place
- internal investigations (non-criminal investigations)

1.6 It also presents challenges as the use of such methods can still interfere with a person's right to respect for their private and family life which is enshrined in Article 8 of the Human Rights Act and the European Convention on Human Rights. The same basic principles, statutory provisions and codes of practice apply to investigative action, and material gathered online, as offline.

1.7 Public Authorities must ensure that any interference with this right is:

- necessary for a specific and legitimate objective – such as preventing or detecting crime
- proportionate to the objective in question, and
- in accordance with the law.

1.8 Whenever you are using the internet to gather intelligence or evidence you must consider whether you are likely to interfere with a person's private and

family life and, if so, whether you should seek authorisation under the Regulation of Investigatory Powers Act (RIPA) prior to undertaking such activity.

1.9 It is also essential to consider the effect of any collateral intrusion on the private and family life of other people not directly connected with the subjectof the research or investigation.

1.10 As such, it is vital that judgement is exercised on a case by case basis prior to commencing any online research or investigations.

1.11 This policy therefore sets out a clear framework for the use of online material, social media and other similar sites during the course of enquiries or investigations.

2 Legal Framework

2.1 Online research and investigation techniques may be affected by any or all of the following legislation:

- Human Rights Act 1998 (HRA)
- European Convention on Human Rights (ECHR)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Investigatory Powers Act 2016 (IPA)
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018 (DPA)
- Protection of Freedoms Act 2012

Human Rights Act / European Convention on Human Rights

2.2 The right most likely to be engaged by staff undertaking online research and investigation is Article 8 which states:

8.1 Everyone has the right to respect for his private and family life, his home and his correspondence.

8.2 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 nationalsecurity, public safety or the economic well-being of the country, forthe prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

2.3 Ensuring that RIPA authorisations are sought, where necessary, and that the material obtained is retained and processed in accordance with the provisions of the Data Protection Act should provide the lawful authority required by Article

8.2 for any perceived interference with Article 8.1.

Regulation of Investigatory Powers Act 2000 (RIPA)

2.4 Under 26(2) of RIPA, surveillance is “directed” if it is covert but is notintrusive and is undertaken:

- for the purposes of a specific investigation or a specific operation
- is likely to result in the obtaining of private information about a person
- is otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.

2.5 Whether or not there is a likelihood of obtaining private information will be a determining factor when considering if an authorisation as directed surveillance will be appropriate.

2.6 Private information is information relating to a person’s private or family life. It can include any aspect of a person’s relationships with others, including professional or business relationships.

2.7 A person may have a reduced expectation of privacy when in a public place but covert surveillance of their activities in public may still result in the obtaining of private information.

2.8 This principle applies equally to the online world, including social media sites, where access controls set by the owner of the information may be a determining factor in considering whether information posted on the internet is publicly available or whether, by applying the access controls, the owner has removed the information from a wholly public space to a more private space where the information could be considered as private.

2.9 Unrestricted open source information is unlikely to fall within the definition of private information.

Protection of Freedoms Act 2012

2.10 With effect from 1st November 2012 formal applications to use covert techniques must have prior judicial approval. In addition, restrictions limiting the use of formal approved surveillance to the investigation which attract a custodial sentence of 6 months or more have been introduced for applications for all surveillance techniques.

General Data Protection Regulation (GDPR) & Data Protection Act 2018 (DPA)

2.11 The GDPR guiding principles are that personal data must be processed fairly, lawfully and transparently; must not be processed in a manner that is not compatible with the purpose for which it was obtained; must be relevant and adequate but not excessive; be accurate and kept up to date; must not be kept longer than is required; and be processed with integrity and confidentiality.

2.12 Much of the information obtained by online research and investigation will meet the definition of personal data. Case law has established that the processing of personal data is capable of interfering with a person's Article 8 right to respect for their private and family life, irrespective of whether the information was obtained under a RIPA authorisation or not.

2.13 Where processing is conducted by an officer with a statutory function with a law enforcement purpose, they shall do so within the provisions of Part 3 of the DPA 2018 (Law Enforcement Processing)

3 Open Source Information

3.1 Most of the information available on the internet is available to any person with internet access. Such information is widely known as open source information.

3.2 Viewing open source information does not amount to obtaining private information because that information is publicly available. This is therefore unlikely to require authorisation under RIPA whether it is done on a one off basis or by repeated viewing.

3.3 Recording, storing and using open source information in order to build up a profile of a person or group of people must be both necessary and proportionate and, to ensure that any resultant interference with a person's Article 8 right to respect for their private and family life is lawful, it must be retained and processed in accordance with the principles of the GDPR.

3.4 In relation to open source material, the following definitions are provided to assist those involved in online research and investigation:

- Open source research – the collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise, to use as intelligence or evidence in investigations.
- Open source information – publicly available information, i.e. anymember of the public could lawfully obtain the information by request or observation.
- Unrestricted sites which can be located via search engines such as Google. No membership, user profile, registration, login process required

to view the data, e.g. Wikipedia.

- The unrestricted, open, public facing sections of partitioned sites which make certain material available to all, but which have other sections or functionality which are only accessible to those who have registered as members and hold a valid login, e.g. social media and social networking sites (SNS's) like Facebook or Twitter; and online trading sites ('OTS's) such as eBay.

3.5 Whilst it is unlikely that the viewing of such information on a repeated basis will amount to surveillance, each site should be assessed on a case by case basis.

3.6 It may not, for example, be proportionate to view a Facebook or Twitter profile of a particular individual on numerous repeated occasions within a short space of time. Persistent study of an individual's online presence could be considered covert surveillance and a RIPA authorisation may need to be considered. Viewings must only be undertaken once with any further proposed viewing considered as targeted surveillance and an authorisation under RIPA may be required.

3.7 This 'first dip' allows the officer to establish basic facts and ascertain whether the information contained within the page is 'open source' or whether security settings have been applied. Officers must be aware that, depending on the nature of the online source, there may be a reduced expectation of privacy where information about an individual is made openly available in the public domain, but in some circumstances privacy implications still apply. This is because the intention when making it available was not for it to be used for covert investigative activity. This is regardless of whether a user has activated privacy settings. See Annex One for further details from the Covert Surveillance and Property Interference Code of Practice (2018) relevant to online covert activity.

3.8 Whenever a social media page is accessed, this should be recorded in a log and the page mirrored. Where mirroring is not possible, screen shots should be taken and retained as evidence and the continuity and storage of such evidence must be recorded.

3.9 Investigative techniques must be within the rules:

- Provenance must be clear and demonstrable
- Continuity must be intact
- Is there any reason a Court may conclude that techniques used, or material gathered, jeopardises the defendant's right to a fair trial.

4 Restricted Access Information

4.1 Access to some of the information on the internet is restricted by the owner, for example a common form of restriction is in social networks where a profile owner may use the privacy settings to restrict the access to online “friends”.

4.2 Privacy settings are covered fully in Section 5 below.

4.3 Viewing restricted access information covertly will generally constitute covert surveillance and, as the information is not publicly available, it is likely that private information will be obtained.

4.4 Under these circumstances an appropriate authorisation under RIPA should be sought prior to undertaking any such surveillance.

4.5 It should be noted that the use of a false persona in an attempt to bypass privacy controls and gain access to restricted information, i.e. by sending a false “friend” request, is expressly forbidden unless this has been approved via a RIPA CHIS application.

4.6 Whenever investigations are undertaken it must be remembered that any online research or investigation leaves a trace or “footprint” which can be tracked back to the council.

4.7 Recording, storing and using restricted access information must be dealtwith in accordance with the principles outlined above in section 3.3.

5 Privacy Settings

5.1 Most social media sites will have a variety of privacy settings that users can apply to restrict information and protect their accounts from others accessing such information.

5.2 Using Facebook as an example, depending on what privacy setting a user chooses, different people can access the account and see some or all of the content.

Public Setting

5.3 All Facebook users can see the account and all of its content, including the user’s “friends”, their timeline and photographs. Non-Facebook users can see photographs and posts published on the account, but not who has “liked” a post or the marital status and geographic location of the user.

“Friends” Setting

5.4 Only those who the user has accepted as Facebook “friends” are able to see the entire content of the user’s page.

Custom Setting

5.5 The user can create lists of specific contacts and Facebook users and

designate them as the audience for, or block them from view of, any posts.

5.6 Of the three options outlined above the only resource normally available to investigators is the public profile, although as indicated in Section 6 below there may be limited occasions where the "friend" profile may become available.

6 Utilisation of Social Media Information

Surveillance using an officer's private account

6.1 If an officer views a user's profile with whom they are not "friends" and where the content is not protected by any privacy settings, then information on this profile can be treated as being in the public domain. Visiting/viewing this profile will accordingly be overt and no authorisation under RIPA will be required.

6.2 If the officer frequently or regularly visits/views the same individual's profile this must be considered as targeted surveillance and an authorisation under RIPA will be required. If the user posts publicly, they may have a reduced expectation of privacy depending on the nature of the online platform. Officers must still consider the privacy implications for using such content as outlined in section 3.7 above.

6.3 Officers may not, under any circumstances, send a "friend" request or attempt to contact the user unless that user is already a "friend" and they have a relationship in a personal capacity. Befriending for the purpose of official investigations will require a RIPA authorisation for CHIS.

7 Conclusion

7.1 The use of social media as an investigation tool is constantly evolving and it is not therefore intended that this policy will cover all eventualities.

7.2 Whilst it is unlikely that any formal RIPA authorisation will be necessary this aspect must be considered by Investigators in accordance with the RIPA Policy and great care must be taken to ensure that there is no interference with a person's right to respect for their private and family life.

7.3 Best practice is to apply the tests of RIPA (proportionality, necessity, reducing collateral intrusion and demonstrating that you have still considered their Human Rights when applying the circumstances) even if formal authorisation is not required, and record the outcome and decision in accordance with the 'Non RIPA' procedure as detailed within the RIPAPolicy.

7.4 Where there is any doubt regarding the use of this policy, advice should be sought from the Information Rights Team.

Annex One

The following is an extract from the Covert Surveillance and Property Interference Code of Practice (2018) relevant to online covert activity. The full code of practice should be read in relation to any consideration of surveillance activity. It is available on the Home Office website at - CHIS Code (publishing.service.gov.uk)

Online covert activity

3.10 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if 19 no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable

expectation of privacy in relation to that information.

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6 of the Code.

***Example 1**: A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

***Example 2**: A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*

***Example 3**: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or 20 operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

3.16 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation.
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 of the Code);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile.
- Whether the information obtained will be recorded and retained.
- Whether the information is likely to provide an observer with a pattern of lifestyle.
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life.

- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s).

- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32 of the Code).

***Example**: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names 21 or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.*