North East Derbyshire District Council

Guidance on the Use of Social Media in Investigations

DRAFT

Background

The Council has an approved Corporate Policy and Procedures Document on the Regulation of Investigatory Powers Act 2000 (RIPA). For all relevant bodies, RIPA arrangements and use fall under the oversight of the Investigatory Powers Commissioner's Office (IPCO), which assumed responsibility from the former Office of Surveillance Commissioners (OSC) in September 2017, and the Council may be subject to a periodic inspection to ensure that it complies with legislation and guidance.

In the reports for the Councils, both 2013-14 and 2014-15, comment was raised on the use of social networks in investigations as follows:

2013-14 report
"This is now a deeply embedded means of communication between people and one that public authorities can exploit for investigative purposes."

"Although there remains a significant debate as to how anything made publicly available in this medium can be considered private, my Commissioners remain of the view that the repeat viewing of individual 'open source' sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity."

"I strongly advise all public authorities empowered to use RIPA to have in place a corporate policy on the use of social media in investigations."

2014-15 report
"Public authorities now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices."

"I repeat my view that just because this material is out in the open, does not render it fair game. The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA and this includes repetitive viewing of what are deemed to be 'open source' sites for the purpose of intelligence gathering and data collation."

"My inspections have continued to find instances where social networking sites have been accessed, albeit with the right intentions for an investigative approach, without any corporate direction, oversight or regulation."

In August 2018, the Home Office issued its Revised Code of Practice covering Covert Surveillance and Property Interference and this now includes a section on 'online covert activity' at paragraph 3.10 onwards and can be found at Appendix 1.

DRAFT

A copy of the full guidance can be found at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

This corporate guidance document has been developed to assist officers in ensuring their investigations are carried out lawfully.

General RIPA Information

The guidance states that:-

> *"The Internet is a surveillance device as defined by RIPA section 48(1). Surveillance is covert 'if, and only if' it is conducted in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is, or may be, taking place.' Knowing that something is happening is not the same as an awareness that it is or may be taking place."*

While activity involving the use of social networks in an investigation may be deemed to be surveillance, within the meaning of RIPA (S.48(2)), not all will require a RIPA authorisation (or qualify for the protection offered through RIPA compliance – i.e. it may not reach the crime threshold).

Most cases which officers investigate will not meet the crime threshold for a RIPA authorisation. RIPA use now not only requires the internal approval of an Authorising Officer but also that of a magistrate.

This test is set out within the Council's RIPA policy.

Where a proposed investigation does not relate to an activity that meets the crime threshold, the Council expects officers to follow a similar procedure for assessment, evidencing necessity / proportionality and internal Authorising Officer review in order to provide a documented trail as a defence in the event of subsequent litigation.

Although failure to obtain appropriate authorisation or undertake a proper assessment does not render surveillance automatically unlawful, it could lead to any evidence obtained being deemed inadmissible and/or civil action taken against the Council / Officers for breach of the subject's right to privacy under Article 8 of the European Convention on Human Rights.

The Convention qualifies this right so that in certain circumstances the Council may interfere in that person's right if that interference is:-

- in accordance with the law;
- necessary; **and**

DRAFT

- proportionate.

Depending upon the circumstances, the IPCO and the Home Office have advised that accessing or use of information found on social media, could be classed as Covert Directed Surveillance or the use of a Confidential Human Intelligence Source (CHIS) on a case by case basis:-

- Covert Directed Surveillance means surveillance which is carried out in such a way that the person(s) subject to it is unaware that it is or may be taking place.
- As a result of the Protection of Freedoms Act, from 1 November 2012 Directed Surveillance authorisations will have a crime threshold applied whereby local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.
- A person is a Covert Human Intelligence Source (CHIS) if they establish or maintain a relationship with another person in order to:-
  - covertly obtain information;
  - provide access to information to a third party; or
  - covertly disclose information obtained by the use of such a relationship and the other person is unaware that the purpose of the relationship is one of the above.

<u>Information on the Internet</u>

Online communication via the internet has, in recent years, become the preferred method of communication with other individuals, within social groups or with anyone in the world with internet access. Such communication may involve web sites, social networks (e.g. Facebook), chat rooms, information networks (e.g. Twitter) and/or web based electronic mail.

Just because other people may also be able to see it or access the information, does not necessarily mean that a person has no expectation of privacy in relation to that information.

Observing, monitoring and obtaining private information can amount to covert surveillance and therefore an interference with a person's right to respect for their private and family life.

Many officers and staff will have considerable experience of using the internet for their own personal online research. However managers should ensure that staff members carrying out online research and investigation for the Local Authority are both competent and appropriately trained. Any online research and investigation leaves a trace or 'footprint' and therefore safeguards need to be put in place to protect staff but

DRAFT

also adequate procedures need to be in place to ensure such interrogation is undertaken lawfully.

DRAFT

Council Guidance

Open Source Research is the collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise, to use as intelligence or evidence within investigations.

Open Source Information is publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation). It includes books, journals, TV and radio broadcasts, newswires, internet WWW and newsgroups, mapping, imagery, photographs, commercial subscription databases and grey literature (conference proceedings and institute reports).

The Council's corporate approach is that it is acceptable for officers to undertake open source research and access open source information for the purposes of investigations / research in respect of individuals or businesses if undertaken properly, in accordance with council policy and in accordance with the law.

Investigations

If an officer during an investigation, deems it necessary and proportionate to use Open Source Research or collate Open Source Information (and such investigation does not meet the crime threshold for authorisation via RIPA), such use must be subject to adequate consideration and authorisation(s) which will depend upon the activity being undertaken.

Recording, storing and using restricted access information, in order to build up a profile of a person or a group of people must be both necessary and proportionate, and it must be retained and processed in accordance with the principles of the GDPR and DPA legislation.

Appendix 3 provides a general guide for officers.

Privacy Controls

The initial interaction involved in the act of bypassing privacy controls (the sending and acceptance of a friend's request) may not by itself, meet the RIPA definition of a "relationship" and will not require authorisation as a Covert Human Intelligence Source (CHIS), but such practise is discouraged. Officers are encouraged to use other means of investigating.

The creation of a false persona involving other "friends", which are also false, in order to effect the deception and secure the information effectively amounts to "legend building" in support of the CHIS and would require proper authorisations. Again this is discouraged.

DRAFT

Under no circumstances should an investigating officer encourage inappropriate, fraudulent or criminal behaviour in order to provoke a response as part of the use of social networking facilities in ANY of the circumstances described above.

Officers must not set up bogus accounts/identities without further discussion with the RIPA Authorising Officer and/or Legal Services and such activity will be discouraged.

Prior Notification

Unless you seek the proper authority from the Magistrates Court for permission to use covert surveillance techniques, prior notification of the use of social media in investigations should be given. Suitable wording can be provided by Legal Services or the Governance Team.

DRAFT

Access to Social Media Accounts

Officers should not use personal or private accounts to access social media for the purposes of investigations.

One specified Corporate Social Media Account will be used for the purposes discussed above. Such account will not use a false identity.

The communications team will monitor the sites although there will be a clear post on the site advising individuals that the site is not monitored and will redirect them to use the customer services email/telephone number.
Such site will only be used to carry out searches and not to comment, friend or "like" certain pages. Officers can screen shot information relevant to their investigation, in accordance with the table set out above and recorded in the table as set out in appendix 2.

When is Authorisation for Social Media Use Required

Research activity does not need to be authorised or recorded **except** where it relates to an investigation by any Service Area. For example, the communications team would not normally need to record their social media usage unless they are requested to access social media on behalf of another service as part of an investigation.

No social media investigations should be carried out without prior knowledge of the relevant Service Manager (where relevant) and authorisation of someone more senior than the investigating officer.

Single visit or casual research on social media does not need to be recorded, however, where there are repeated visits to a premises or visits to a specific web page or facebook page a log should be retained and initialled by the Service Manager to confirm their authorisation for the activity.

The following should be recorded on a log with the following information:

- Officer carrying out the research
- Target of the investigation
- Date/time of viewing
- Information obtained from social platform
- Why it was considered that the viewing was necessary
- Pages saved and where saved to
- Authorisation from the Service Manager (or substitute)

The template log attached to this policy at appendix 2 should be used unless the information identified above can be recorded on a team's own "working" system (for example ECINS) so long as the information can be effectively extracted for the purposes of reporting to the IPCO or Members.

DRAFT

Logs will be reviewed quarterly by the Governance Manager on behalf of the Monitoring Officer and anonymised statistics will be reported to Members annually as part of the RIPA report.

Advice to Officers

As noted elsewhere in this guidance document, there are some grey areas over the legitimate use of social networking in investigations and the IPCO themselves have recognised that "there is a fine line between general observation, systematic observation and research."

If an Officer is considering the use of social networking for such activity, or is uncertain as to how to proceed, then further advice on the guidance and the potential RIPA requirements may be obtained from:-

- RIPA Authorising Officers
- Monitoring Officer
- Governance Manager
- Legal Services

Associated Documents

This guidance is linked to a number of other Council documents which are available to staff via the Extranet:-

- RIPA Policy and Procedures Document
- Social Media Management Guidance – from Communications
- Policy on Social Networking – from Human Resources
- Links to Home Office Statutory Codes of Practice online
- Links to Office of the Surveillance Commissioners' Guidance Procedures online
- Links to RIPA forms online for covert surveillance; CHIS and acquisition and disclosure of communications data;
- Corporate RIPA Training.
- Further information on the ICO Employment Practices Code may be obtained from the Information Commissioner's Office website:- https://ico.org.uk/media/fororganisations/documents/1064/the_employment_practices_code.pdf

DRAFT

Appendix 1 – Extract from Home Office Code of Practice - Covert Surveillance and Property Interference

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 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.

DRAFT

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.

***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.

DRAFT

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 above);
- 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).

***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.*

DRAFT

Extract from Home Office Code of Practice - Covert Human Intelligence Sources

Online Covert Activity

4.11 Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites such as an online news and social networking service, or more private exchanges such as e-messaging sites, in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation. A directed surveillance authorisation should also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

4.12 Where someone, such as an employee or member of the public, is tasked by a public authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:

- An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person.
- Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose.
- Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

4.13 A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of a public authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

***Example** 1: An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed and a CHIS authorisation need not be sought.*

***Example** 2: HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases.*

DRAFT

The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

4.14 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for an officer of a public authority or a CHIS to engage in such interaction to obtain, provide access to or disclose information.

***Example** 1: An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity he “follows” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed and no CHIS authorisation is needed.*

***Example** 2: The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation.*

4.15 When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for authorisation. Full consideration should be given to the potential risks posed by that activity.

4.16 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 6.13 of this code should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or authorising officer, and the extent to which this may impact on the effectiveness of oversight.

4.17 Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved. (See also paragraph 3.23)

DRAFT

Appendix 2

LOG – Accessing Social Media (see notes below)

Officer and designation accessing social media	***Date/time***	***Social media type***	***Reason/purpose/why is it necessary?***	***Means of notification of access to information***	***Information retained/used***	***Action taken e.g. CPW, prosecution, injunction***	***Senior officer signature***

DRAFT

Appendix 3

Notes (if in doubt seek advice)-

Nature of Activity	***Assessment Required***	***Log/Records Required***	***Possible RIPA Authorisation***
Communications Research - browsing (monitoring) 3rd party posts on social networking sites / feeds (e.g. Facebook ,Twitter, Instagram etc.) solely for the purposes of identifying comments (positive or negative) about the Council and its activities (as is also undertaken for newspapers) is a research activity for sharing information with our residents and businesses from partner organisations such as Derbyshire Police, traffic/weather updates, community events etc.	***No***	***No***	No
Casual (one-off) examination of public posts on social networks as part of investigations undertaken	***No***	***Yes*** ***Simple form listing sites/targets***	***No***
Repetitive examination / monitoring of public posts as part of an investigation	***Yes*** ***Authorisation from*** Officer more senior than the investigating officer	***Yes***	***May be classed as Directed Surveillance***. Seek advice if unsure.
Examination / use of any ostensibly 'private' mechanisms on social networks (e.g. as a 'friend' on Facebook, use of 'private' messaging facilities on Twitter, etc.):- • within an existing relationship where the parties are known to each other, but information that is	***Yes*** ***Authorisation from Service Manager***	***Yes***	***Yes*** Directed Surveillance or the use of a CHIS

DRAFT

freely obtained is used or passed on to an appropriate area for use in an investigation • through a new relationship set up in an open manner (i.e. in the name of the Council)			
Any Covert activity such as the following circumstances: • where a relationship is set up in a 'covert' manner specifically to obtain information • a person known to the subject becomes a 'friend', etc. specifically for the purposes of the investigation • a person becomes a 'friend', etc. in a false or misleading name • where a dialogue is entered into in order to elicit information for the investigation with the subject remaining unaware (as this may be classed as entrapment)	***Yes*** ***Must inform RIPA authorising officer/Monitoring Officer***	***Yes***	***Yes*** Directed Surveillance and/or the use of a CHIS

DRAFT