# Nottingham City Council
# Guidance relating to Online Research and Investigation

**This document is intended to provide guidance to Local Authority staff engaged in research and investigation across the internet, including social media.**

**If you would like any advice regarding the guidance provided in this document please contact the Data Protection Officer or the Information Compliance Team, Legal and Governance, Nottingham.**

This guidance for Online Research and Investigation is provided to assist staff members engaged in research and investigations that require the use of the internet. The document is circulated to promote good and consistent practices across the Local Authority.

This document must be considered together with the Covert Human Intelligence Sources code of practice and the Covert Surveillance and Property Interference code of practice 2018 (some sections have been referred to in this guidance).

It is important to emphasise that whether or not any RIPA authorisation is required by a Local Authority officer will depend on the precise circumstances of any particular case.

**Senior Responsible Officer**:
Malcolm R Townroe – Director of Legal and Governance

This guidance focuses on how the principles set out in legislation apply to the use of the internet, including social media, as an investigative tool. It does not replace statutory guidance. Each activity should be considered on a case by case basis.

Covert investigative techniques likely to interfere with a person's Article 8 rights should be used only when necessary and proportionate. Both the Regulation of Investigatory Powers Act (RIPA) and the General Data Protection Regulation (GDPR) 2016/679 and the Data Protection Act 2018 (DPA) provide a framework for ensuring that such action is lawful and in accordance with the European Convention of Human Rights (ECHR) and the Human Rights Act (HRA). RIPA Codes of Practice provide statutory guidance on the use of some of these techniques.

Online research and investigation is a powerful tool against crime. It also presents new challenges to law enforcement as the use of such a tool 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 1998 and ECHR.

Investigators working for Nottingham City Council 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;
- in accordance with the law.

Whenever you are using the internet to gather intelligence or evidence you must consider whether you are likely to interfere with a person's right to respect for their private and family life and, if so, whether you should seek authorisation under RIPA for your conduct. The principles in this guidance have been prepared to help you identify if such authorisation is appropriate.

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 subject of the research or investigation.

**Case by case judgement is vital when researching or investigating online.**

**Guiding Principles – Overview and operational risk considerations**

**Overview**

- 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, does not necessarily mean that a person has no expectation of privacy in relation to information posted on the internet. Using covert techniques to observe, monitor and obtain private information can amount to an interference with a person's right to respect for their private and family life. Authorisation regimes, such as RIPA, must be considered although RIPA is not the only legislation which can render such interference lawful.
- **Any online research and investigation leaves a trace or 'footprint'**. A decision will therefore need to be made as to whether you wish to ensure that your research is non-attributable i.e. cannot be traced back the Local Authority or to identifiable individuals, or whether you are happy for it to be attributable i.e. capable of being traced back to the Local Authority.
- Non-attributable research and investigation must be carried out on equipment that cannot be attributed to the Local Authority or identifiable individuals, just as attributable research and investigation must be carried out on attributable equipment. Carrying out any attributable activity on non-attributable equipment runs the risk of compromising the equipment and any operational activity which has been conducted on it.
- It is recommended that attributable research and investigation is restricted to publicly accessible search areas e.g. maps, street views, local authority sites, auction sites, etc. and websites which have no requirement to register details in order to gain access.
- It is acknowledged that 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.

## Use of a false persona

It is recognised that there will, for **covert** online research and investigation, be a requirement to create and use false persona accounts to gather information. The creation of a false persona for the purposes of online research and investigation is likely to require a RIPA.

A log, recording the time, date, user and the purpose, should be maintained for each use of a false persona.

The OSC procedures and guidance document 2014 (now IPCO) states at paragraph 288.3 "it is not unlawful for a member of the public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without Authorisation.

Using photographs of a person without their permission to support the false identity infringes other law.

- Most of the information available on the internet is available to any person with internet access, either freely or for payment. Such information is widely known as open source information.
- Viewing open source information, by attributable means, does not amount to obtaining private information because that information is publicly available. This is therefore unlikely to require authorisation under RIPA. However, the repetitive viewings of what are deemed to be open sources for the purposes of intelligence gathering or data collection may require an authorisation under RIPA and advice should be sought on individual cases.
- Recording, storing and using open source information in order to build up a profile of a person or a 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 General Data Protection Regulation 2016/679 Data Protection Act 2018.

## Open source

**Definitions**

- 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 within investigations.
- Open Source Information - 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).

## Restricted access information

- Access to some of the information on the internet is restricted by its "owner". A common form of such restriction is in social networks where a profile owner may use the privacy settings to restrict access to online "friends".

- 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. Authorisation as directed surveillance should be sought in these circumstances.
- 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.
- The initial interaction involved in the act of bypassing privacy controls (the sending and acceptance of a friend's request) may be minimal. In many cases it is considered unlikely that this, by itself, will meet the RIPA definition of a "relationship" and will not require authorisation as a Covert Human Intelligence Source (CHIS). However, much work may have had to be conducted to get to that stage without arousing suspicion. In addition, it may be difficult to predict how or at what pace that "relationship" will need to develop. If it is intended or considered likely that direct one to one interaction with another person will go beyond the initial request/acceptance it will be appropriate to seek authorisation as a CHIS. 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.
- Considerations of the potential for any subsequent interaction, that would qualify as a "relationship", should be appropriately documented as part of the decision making process. This should include the reasons for any decision not to authorise the use of the undercover online Local Authority officer undertaking the activity as a CHIS and contingency provisions for authorisation if subsequently considered appropriate.
- Although this minimal initial interaction will not require authorisation as a CHIS it is considered good practice for friends' requests to be sent by a trained undercover Local Authority officer.

## The Law – Overview

Online research and investigation techniques may impact on all or any of the following:

- Human Rights Act 1998 / European Convention on Human Rights
- Regulation of Investigatory Powers Act 2000
  - Part I – Interception of Communications and the Acquisition of Communications Data
  - Part II – Surveillance and Covert Human Intelligence Sources
- Computer Misuse Act 1990
- General Data Protection Regulation 2016/679 and the Data Protection Act 2018

## Human Rights Act / European Convention on Human Rights

Both of these provide a number of fundamental rights which are central to all actions of law enforcement.

The right most likely to be engaged by officers and 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 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*.

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.

## Directed Surveillance

Under section 26(2) of RIPA, surveillance is 'directed' if it is covert but not intrusive and is undertaken

- **for the purposes of a specific investigation or a specific operation; and**
- **is likely to result in the obtaining of private information about a person; and**
- **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 Part II to be sought for the carrying out of the surveillance.**

The likelihood of obtaining private information will be one of the determining factors when considering whether authorisation as directed surveillance is appropriate.

**Private Information**

**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.**

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.

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 private.

**Covert Human Intelligence Source (CHIS)**

Under section 26(8) of RIPA, a person is a CHIS if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything below:

- **he covertly uses such a relationship to obtain information or to provide access to any information to another person; or**
- **he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.**

The making and acceptance of a friends request may constitute some interaction with a person; however it is minimal and is unlikely to satisfy the definition of a relationship. Authorisation as a CHIS need only be sought when it is anticipated that the relationship will be developed beyond this initial contact.

**Computer Misuse Act 1990**

Sections 1-3 of the Computer Misuse Act 1990 introduced three criminal offences:

- **unauthorised access to computer material;**
- **unauthorised access with intent to commit or facilitate commission of further offences; and**
- **unauthorised modification of computer material.**

The basic offence is to attempt or achieve access to a computer or the data it stores, by inducing a computer to perform any function with intent to secure access. The precondition to liability is to be aware that the access attempted is unauthorised. Thus the following activities may constitute the offence:

- **to use another person's username and password without lawful authority or consent to access data or a program;**
- **to alter, delete, copy or move a program or data;**
- **to impersonate that other person using e-mail, on line chat or other web based services.**

**Retention and processing of information. General Data Protection Regulation 2016/679 and the Data Protection Act 2018 and other relevant legislation / guidance**

The GDPR and the DPA deals with how material obtained must be handled. The Data Protection guiding principles are that personal data must be processed fairly and lawfully, 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 and must not be kept longer than is required.

Much of the information gathered 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 the authority of RIPA or otherwise.

For any interference with a person's Article 8 rights resulting from the processing of such information to be in accordance with the law, as required by Article 8.2, it is therefore essential that all information so obtained is processed in accordance with the principles of the GDPR and DPA.

Please refer to the Nottingham City Council's Data Protection Act policy and Guidance for further information.

The retention of material obtained in a criminal investigation is also subject to the provisions of the Criminal Procedure and Investigations Act 1996 and its associated Code of Practice. This Act sets out a number of statutory criteria for the handling and retention of such material.

**Covert Surveillance and Property Interference Code of practice – 2018 – Online Covert Activity Page 18.**

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.

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.

***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
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:

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 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.*

*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 identity12, 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.*

**Covert Human Intelligence Source code of practice 2018 - Page 23**

***Online Covert Activity***

*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. 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.*

## Using the Internet for Investigative Purposes

1. Staff using the internet for investigative purposes must not use their own personal devices (PC, laptop, tablet, smart phone etc.) as a means of accessing the internet. It is important to bear in mind that all internet activity leaves a footprint. Websites routinely gather IP addresses and in some cases use data trawling software to gather more intrusive information from the device used, which is then potentially traceable.

2. Staff must not, under any circumstances, use their own personal Social Networking Sites (SNS) profiles or other online accounts to undertake investigative research. There have been cases where such practices have resulted in the safety of officers and their families being seriously compromised.

3. In order that the Local Authority can effectively manage online overt and covert profiles/accounts i.e. SNS profiles, Auction Site accounts, email accounts etc., which have been created for investigative purposes using false details, details of the investigation must be entered in a Local Authority log.

4. If a Local Authority officer wishes to look at a SNS site covertly i.e. by setting up false identity they should use a Nottingham City Council computer and use a Nottingham City Council social networking account. Any monitoring of SNS accounts should be recorded in a log.

5. When setting up a covert online account staff must not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site.

6. It should be noted that the viewing of open source material via the internet, by overt means, will not usually amount to obtaining private information as the material is publicly available. It is therefore unlikely that activity of this nature will require an authorisation under RIPA, unless there are repeated viewings, in which case legal advice should be sought.

7. Staff engaged in open source SNS research must not attempt to defeat privacy settings by submitting friend's requests to subjects in order to gain access to the information held in the private areas of their profiles. Such activity, dependent on the objective, would require at least a directed surveillance authority (DSA) and may require a CHIS authority if any form of interaction is required. Advice should be sought from Legal/ Information compliance if there is a need to deploy this tactic.

8. Staff with access to covert SNS profiles must not befriend other SNS users in order to build the credibility of their profiles. Such enhancements are not necessary for open source research as a covert profile will only become visible if some form of interaction takes place i.e. a friends request is submitted. Furthermore it is important to bear in mind that such activity would represent a breach of the ECHR as it effectively enables the Local Authority to access the personal information of unsuspecting SNS users without the necessary justification.

9. Staff conducting open source research must not engage in any form of interaction with other internet users irrespective of the forum i.e. any form of instant messaging, email etc.

10. The Covert Surveillance and Property Interference code of practice 2018 and the Covert Human Intelligence Sources Code of practice - 2018 should be adhered to when carrying out criminal investigations on the internet.

**Advice should be sought from Legal and Governance as to whether a RIPA authorisation is required.**