Internet & Social Media Research & Investigations

Procedure

Revision	Revision Date
1.	October 2022
2.	October 2023

NORTH NORFOLK DISTRICT COUNCIL

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 techniques has become a productive method of obtaining information to assist North Norfolk District Council with its regulatory and enforcement functions. It can also assist with other functions such as, service delivery issues and debt recovery. 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 Human Rights Act (HRA) and other operational risks.

1.3 North Norfolk District Council is a Public Authority in law under the Human Rights Act 1998, and as such, the staff of the authority must always work within this legislation. This applies to research on the internet. Just because it may seem easier to carry out internet research does not mean that it should take place without justification.

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 to respect for their private and family life is lawful, the material must be retained and processed in accordance with the principles of the General Data Protection Regulations (GDPR).

2. Scope of Procedure

2.1 This procedure is a restricted document for use by North Norfolk District Council Council staff only. It should not be published or distributed or disclosed under Freedom of Information Requests. However, it can be used for both Criminal and Civil proceedings.

2.2 This procedure establishes North Norfolk District Council's corporate standards and instructions, which will ensure that all online research and investigations are conducted lawfully and ethically to reduce risk. It provides guidance to all staff, when they are engaged in their official capacity of the implications and legislative/best practice framework associated with online internet and social media research. It will also ensure that the activity undertaken, and any evidence obtained will stand scrutiny.

2.3 This procedure takes account of the Human Rights Act 1998, Regulation of Investigatory Powers Act (RIPA) 2000 August 2018 Codes of Practice, Criminal Procedures Investigations Act (CPIA) 1996, General Data Protection Regulations (GDPR), Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence (March 2012), National Police Chiefs Council (NPCC) Guidance on Open-source Investigation/Research. It also has regard ~~follows~~ to the guidance and best practice advice

documented within the Office of Surveillance Commissioners (OSC) Procedures and Guidance July 2016. ~~The OSC is now replaced by the Investigatory Powers Commissioner's Office (IPCO). However, t~~The Procedures and Guidance document has now been withdrawn by IPCO. The Council will have regard to any revised guidance as and when it is issued by IPCO. ~~is still current.~~

2.4 This procedure will be followed at all times and should be read, where required with the RIPA Codes of Practice and other relevant policies mentioned in this document. Should there be any queries, advice can be sought from the SRO or Monitoring Officer. Where activity meets the RIPA criteria the RIPA policy and procedures must be followed.

2.5 Not adhering to policy and procedures could result in members of staff being dealt with through the Council's disciplinary procedure.

3. Risk

3.1 Staff must be aware that any activity carried out over 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 North Norfolk District Council from being 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". 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".

3.2 There is also a risk of compromise to ongoing covert investigations and tactics; therefore, the activity should be conducted in a manner that does not compromise any current or future investigation or methods.

3.3 To reduce these risks, risk assessment should be standard practice and carried out in all cases prior to and during any open-source internet and social media research. This will include whether or not you wish to ensure that the research is non-attributable i.e. cannot be traced back to North Norfolk District Council, such as authorised RIPA activity. (See section 10)

3.4 Risk assessments will be recorded within the relevant documentation appropriate to the type of research being undertaken.

3.5 If the RIPA procedure is engaged with regard to CHIS activity (see section 10.12), a risk assessment is a requirement of the Codes of Practice.

3.6 General routine enquiries (see section 9) will rarely pose a risk as they will be carried out in an open official capacity, as opposed to a covert capacity. They will normally be carried out on networked computers attributable to North Norfolk District Council.

3.7 Using trained staff (see section 24) to undertake certain online research will reduce risks. The use of untrained staff will be a risk-based decision by the departmental managers based on the skills and experience of the individual undertaking the research and the nature and level of the research required.

4. Private Information and Privacy

4.1 Due to the ease with which internet research can be undertaken and the amount of information available, it is easier to breach someone's privacy on the internet. This information is likely to meet the definition of personal data and therefore the usual General Data Protection Regulations (GDPR) apply.

4.2 Whenever a public authority intends to use the internet as part of an investigation, they should consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. This should be an ongoing assessment. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case.

4.3 **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. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a Directed Surveillance authorisation is appropriate".

4.4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate. (Sec 3.5 RIPA Codes of Practice Aug 18)

4.5 This is likely to apply to social media sites whether or not access controls have been activated. The other consideration is that the person subject of the investigation has little or no control over the publication of their personal information by other people or organisations.

4.6 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 such as Twitter, are also less likely to hold a reasonable expectation of privacy in relation to that information.

4.7 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way,

recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites. (Sec 3.4 Aug 18 RIPA Codes)

4.8 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. (Sec 3.13 RIPA Codes of Practice 2018).

4.9 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. (Sec 3.15 RIPA Codes of Practice Aug 2018).

4.10 As can be seen, it is not only the obtaining of the private information, it is how it is used and managed afterwards. Using the information and analysing the data to make decisions will impact on privacy.

4.11 Identifying specific objectives and conducting a privacy assessment prior to (if possible) and during internet research will reduce the level of intrusion and enable proportionality to be assessed. This assessment should be documented.

5. Collateral Intrusion

5.1 Collateral intrusion is the interference with the private and family life of persons who are not the intended subjects of the research. Measures should be taken, wherever practicable, to avoid or minimise interference with the private and family life of those who are not the intended subjects. Where such collateral intrusion is unavoidable, the activities may still be authorised providing it is considered proportionate to what is sought to be achieved. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

5.2 Any collateral intrusion should be kept to the minimum necessary to achieve the specific objectives of the research.

5.3 All types of research should therefore include an assessment of the risk of any collateral intrusion, and details of any measures taken to limit and manage the intrusion. This will form part of the procedure if RIPA is engaged.

5.4 If for any reason it is intended to access social media or other online account to which an employee of North Norfolk District Council has been

given access with the consent of the owner, this authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for either a Directed Surveillance authorisation or some other form of authorisation such as a Non RIPA authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward. This guidance is contained in the RIPA Aug 18 Codes. If this is the case advice should be sought from the RIPA SRO or RIPA Authoriser.

6. Necessity / Justification

6.1 To justify the research, there must be a clear lawful reason, and it must be necessary to undertake the internet research. Therefore, the reason 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. Therefore, an explanation of why it is necessary to use covert research techniques instead of other conventional enquires will need to be considered. Should the research fall within RIPA activity, the RIPA authorisation deals with this criteria for it to be lawful. (See section 10)

7. Proportionality

7.1 Proportionality involves balancing the intrusiveness 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. What is the benefit to carrying out the activity? How will the benefit outweigh the intrusion?

7.2 The activity will not be proportionate if it is excessive in the circumstances of the case. The extent and depth of the enquiries should cause the least possible intrusion on the subject and others. It would also not be proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

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

7.4 There should be an ongoing assessment with regard to necessity and proportionality which should be documented when considered. If the research is no longer necessary or proportionate which could be due to the intrusion out weighing the benefit to the enquiries, the activity should end.

8. Types and levels of Enquiries

8.1 Enquiries will be treated on a case by case basis and will fall into one of the three categories below:

1. **General routine enquiries**

2. **Non RIPA Directed Surveillance activity (requires authorising internally)**

3. RIPA activity (requires authorising internally and approved by a Magistrate)

8.2 The nature of the online activity may evolve during the course of the enquiries; therefore, staff must continually assess and review their activity on a case by case basis to ensure it remains lawful and the correct policies and procedures are followed. Further information regarding each type of enquiry is detailed below.

9. General Routine Enquiries

9.1 The general observation duties of many law enforcement officers and other public authorities do not require RIPA authorisation, whether covert or overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation. (3.33 Aug 2018 RIPA Codes of Practice)

9.2 These types of enquiries consist of attributable, overt, initial non-repeated research. This includes any research that is intended to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies. Some examples are shown below:

- Monitoring social media re a future event for resource implications.
- Initial research to proactively identify how many persons are advertising waste collection via social media to tackle illegal waste (fly-tipping).
- Initial enquiries to corroborate a complaint of a regulatory nature.
- Enquires relating to safeguarding issues.
- Initial enquiries to establish whether a suspect in an enforcement investigation has an online presence to assess whether there is intelligence or evidence available?
- Initial enquiries to trace a debtor.

9.3 General routine enquiries will not normally engage the RIPA procedure as they are open and transparent and not normally repeated. They will normally be carried out using North Norfolk District Council's networked computers via open search engines such as Google, and use North Norfolk District Council's official social networking profiles (either corporate or departmental), such as Facebook.

9.4 North Norfolk District Council's networked computers should be used for general routine enquiries which are non-intrusive or of a covert nature such as RIPA operations. A non-attributable computer or laptop should be used for online activity that is covert or may pose a risk to current or future investigations.

9.5 Depending on the circumstances, if having carried out these types of

enquiries it is decided to monitor individuals via repeated viewing of their online presence as part of an ongoing operation or investigation, the RIPA or Non RIPA procedure should be considered. Any decision not to use those procedures should be documented with the rationale for the decision.

9.6 **Level of Authority**

Prior to commencing general routine enquiries on the internet, Senior Environmental Protection Officer or Senior Public Protection Officer approval will be required. This should be documented within the case file notes.

10. Non RIPA Directed Surveillance or CHIS Activity

10.1 Where covert activity (which would include internet research) that does not meet the RIPA threshold but is still required to be carried out by the Public Authority, it has been made clear that to protect the authority, it should be carried out under a procedure as close to that of the RIPA procedure (Sec 211 and 212 in the OSC Procedures and Guidance 2016.).

10.2 The fact that particular conduct may not be authorised under RIPA does not necessarily mean that the actions proposed cannot lawfully be undertaken, even though without the protection that an authorisation under RIPA would afford.

10.3 When it is decided to use covert surveillance without the protection of RIPA it would be prudent to maintain an auditable record of decisions and actions.

10.4 This type of activity will amount to carrying out directed covert online surveillance of a person or group, which is likely to obtain private information about anyone. However, the incident or reason does not relate to a criminal offence which carries 6 months imprisonment or the sale of alcohol or tobacco to children. An example would be in connection with serious disciplinary investigations.

10.5 This also amounts to CHIS activity which does not relate to the prevention and detection of crime or disorder. (See CHIS Section below 11.12 to 11.29)

10.6 **Level of Authority**

In these instances, section 21 of the RIPA Policy should be followed. This will require a Non RIPA application form to be completed which will need authorising internally as per the procedure and signed off by the Authorising Officer (Assistant Director for Environment and Leisure Services).

11. RIPA Activity

11.1 The two relevant areas of RIPA are:

- **Directed Surveillance**
- **Covert Human Intelligence Source (CHIS)**

11.2 **Directed Surveillance** in the context of open-source internet and social media research is **covert surveillance**, which is **not an immediate response** and is undertaken **for a specific investigation or purpose** which is **likely to result in the obtaining of private information about any person.**

11.3 To meet the RIPA criteria, for Local Authorities the serious crime criteria applies which means that the investigation must relate to a criminal offence which can receive a sentence of 6 months imprisonment or relate to the sale of alcohol or tobacco to children.

11.4 **Definition of surveillance** includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

11.5 A computer is a surveillance device and depending on the circumstances, repeated viewing of social media is likely to meet the test of monitoring, which in-turn will amount to surveillance.

11.6 The RIPA Codes of Practice at 3.12 now provide advice re **covert**. "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.

11.7 The Codes of Practice state "Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate" (See Private Information and Privacy section 4).

11.8 When assessing whether a RIPA authority is required, the same principles applied to normal operational tactics will need to be applied to the intended online activity. There is no difference between surveillance in a public place or surveillance on the internet. If the RIPA criteria is met, an authorisation will be required and approved by a Magistrate.

11.9 The Directed Surveillance Codes of Practice at Sec 3.16 provides the following guidance. 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.

11.10 Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation is likely to result in the obtaining of private information about a person or group, and the investigation relates to a criminal offence which can receive a sentence of 6 months imprisonment or relate to the sale of alcohol or tobacco to children, an authorisation for directed surveillance should be considered and the RIPA policy and procedure will apply.

11.11 If it amounts to directed surveillance except for the fact it does not relate to a criminal offence which can receive a sentence of 6 months imprisonment or relate to the sale of alcohol or tobacco to children, an internal authorisation for surveillance outside of RIPA should be considered. (See Sec 11 Non RIPA Directed Surveillance or CHIS Activity)

11.12. **Covert Human Intelligence Source (CHIS)**

11.13 There is a considerable amount of information on the internet associated with illegal activity such as, unlicensed operators and fly-tipping offenders advertising through social media. To successfully obtain sufficient evidence and intelligence, it may be necessary to covertly communicate with suspects online. This is likely to require a CHIS authorisation.

11.14 The guidance relating to online covert CHIS activity is in the RIPA CHIS Codes of Practice. The below information is taken from the codes.

11.15. **Definition of a CHIS**

A CHIS is a person who establishes or maintains a personal or other relationship with a person for the purpose of covertly using the relationship to obtain information, or provide access to any information to another person, or covertly discloses information.

11.16 A purpose is covert, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

11.17 Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. Accordingly, any manipulation of a relationship by a public authority (e.g. one party having a covert purpose on behalf of a public authority) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.

11.18 The lawful criteria for CHIS is **prevention and detection of crime and prevention of disorder** and the offence does not have to have a sentence of 6 months imprisonment. If the enquiry was not for this purpose such as safeguarding or a disciplinary issue it would amount to CHIS activity outside of RIPA which should be authorised under that procedure. (See Sec 9 Non RIPA Directed Surveillance or CHIS Activity)

11.19 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 (as an official rather than private individual) 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. (Sec 4.11 CHIS Aug 18 Code of Practice)

11.20 Regarding any contact, the person must know the true identity and in what capacity are they being contacted. If it is not made clear that it's an official capacity from the relevant department etc. it will be a covert relationship. Therefore, befriending someone using a personal profile to obtain information from them and report back to North Norfolk District Council is covert. This should not take place. (See Use of Own Personal Accounts section 17)

11.21 This would equally apply to using a member of the public as it would to a member of North Norfolk District Council staff making the contact. The Codes of Practice at 4.12 state "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.
- 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.

11.22 The Codes of Practice also provide advice as to whether registering with a site etc. is establishing a relationship. At 4.~~13~~31 it states "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.

11.23 **Example from the Codes of Practice:** 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.

11.24 **Example from the Codes of Practice:** 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.

11.25 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. (Sec 4.~~14~~32 Codes of Practice)

11.26 **Example from the Codes of Practice:** ~~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.~~ An officer who has maintained a false persona uses that persona to send 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 likely to be appropriate in respect of the proposed covert monitoring of the site if the activity is likely to result in obtaining private information. Once accepted into the group it becomes apparent that further interaction is necessary: this should be authorised by means of a CHIS authorisation.

11.27 The above scenario would fit an investigation into an unlicensed seller of exotic pets that only sells through a closed group.

11.28 Any decision to covertly communicate online without authorisation would need to be documented with the rationale for the decision.

11.29 Should it be necessary to covertly engage with subjects online advice should be sought from the SRO or Monitoring Officer.

11.30 **Level of Authority**

Where the research and covert activity meets the RIPA criteria, the activity cannot take place unless authorised by a RIPA Authorising Officer and then approved by a Magistrate. The RIPA application and authrisation process detailed within the RIPA policy will be followed.

12 Errors

12.1 It is important that staff follow all policy and procedures to ensure that if the activity amounts to RIPA activity is properly authorised. This is due to the fact that there are implications for North Norfolk District Council if the activity is deemed to be an error as detailed in the RIPA Codes of Practice and the Council's RIPA Policy. The content is replicated below.

12.2 Proper application of the surveillance provisions in the RIPA codes and this policy should reduce the scope for making errors.

12.3 **Relevant Error**

12.4 An error must be reported if it is a "relevant error". A relevant error for is any error by a Public Authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act (RIPA).

12.5 Examples of relevant errors occurring would include circumstances where:

- Surveillance activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

12.6 Errors can have very significant consequences on an affected individual's rights. All relevant errors made by Public Authorities must be reported to the Investigatory Powers Commissioner by the Public Authority that is aware of the error as soon as reasonably practicable and a full report no later than ten working days. The report should include information on the cause of the error; the amount of surveillance conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

12.7 **Serious Errors**

12.8 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

12.9 It is important that all staff involved in the RIPA process report any issues, so they can be assessed as to whether it constitutes an error which requires reporting.

13. Reviewing the Activity

13.1 During the course of conducting the internet open-source research, the nature of the online activity may evolve. It is important staff continually assess and review their activity to ensure it remains lawful and compliant. Where it evolves into RIPA or non RIPA activity, the respective procedure which takes account of reviews should be followed. If in doubt, seek advice.

14. False Accounts

14.1 It is recognised that there may be a requirement to create and use false identity accounts to gather information for certain covert online research and investigations.

14.2 False identity accounts are accounts on social media sites that appear to be genuine. They provide basic login details, and may include photographs, a 'legend' and other information that makes them appear genuine. These are generally created for conducting more intrusive online activity which is likely to engage the RIPA procedure.

14.3 The creation of a false identity account for the purposes of online research and investigation does not, in itself, require authorisation under RIPA. Although it is likely to breach the terms and conditions of some sites, particularly social networks. The use of a false identity account in relation to a covert investigation is likely to require authorisation under RIPA, dependent upon the activity.

14.4 Should it be necessary to create a false account, it should only be used in conjunction with a stand-alone non-attributable computer or laptop (not networked to North Norfolk District Council) which is used for those purposes.

14.5 A covert account should not be used for general enquiries unless authorised by the SRO or RIPA Authoriser and justified in writing.

14.6 No staff should create a false account without the permission of the SRO or RIPA Authoriser and staff using the accounts will need to have attended some form of suitable Open-source Internet Investigation training course that deals with these issues.

14.7 A record should be maintained by the RIPA Co-ordinator of all false accounts. This enables the false identity to be registered which should only be used by that individual officer. It also enables North Norfolk District Council to have oversight of which departments hold false identity accounts.

14.8 Any department that has created false accounts must also complete a record for each use of a false identity which records the time, date, user and the purpose. This will assist with oversight.

14.9 Use of the false identity within an investigation must be authorised in writing by the RIPA Authoriser to ensure that its use is authorised and lawful. Where the activity engages RIPA or non RIPA Directed Surveillance, the relevant procedure will be followed regarding authorisation. It will also be necessary to liaise with the IT department.

15. Use of Official Organisation / Departmental Social Media Accounts

15.1 When conducting internet enquiries or investigations, some will be carried out through genuine open-source techniques and openly available search engines such as Google (open site), and others will be carried out through some form of registration (closed sites) such as, social networking sites, for example Facebook. In the latter, you would have to join Facebook and use the membership password and profile to have access. Having logged on the site, the investigator is able to research the subject of the investigation and obtain a considerable amount of additional information such as, names, addresses, images and friends etc., by accessing the open content held on friends or colleague's pages. This information would not be available via a Google search and is considerably more intrusive.

15.2 North Norfolk District Council and some departments have their own membership to some social media networking sites such as Facebook. It is through this organisation's membership profile that access should be gained for general routine enquiries (see section 9) as they are open and transparent, not normally repeated and therefore do not engage the RIPA criteria. They should be used to carry out research using attributable computers. They should not be used on a non-attributable computer as it may pose a risk of compromising the equipment and covert operations.

15.3 If other social networking sites are identified which are likely to require some form of internet searches, then an approach should be made via management to the IT department with a view to setting up a Council profile which can be used following the same principles as above.

16. Standalone Non-Attributable Computers

16.1 As mentioned earlier, North Norfolk District Council staff must be aware that any activity carried out over the internet leaves a trace or footprint which can identify the organisation carrying out the enquiries and the device used.

16.2 Network computers will be operating on the internet with static Internet Protocol (IP) addresses and other identifying features which can reveal information about the device and organisation, and the activity undertaken whilst visiting webpages.

16.3 Standalone non-attributable computers or laptops do not normally use the usual network internet connection. They will normally operate on a separate broadband/IP address known as dynamic IP addresses and difficult to trace to North Norfolk District Council.

16.4 A log book should be retained with each non-attributable computer or laptop in which details of all usage must be recorded. The RIPA Co-

ordinator will be responsible for ensuring they are completed correctly.

16.5 Under no circumstances should standalone non-attributable computers or laptops be used for personal use and North Norfolk District Council policy and guidance relevant to computer use will still apply.

16.6 The IT department will be responsible for maintaining the computers or laptops, particularly with regards to software and antiviral software updates.

17. Use of Own Personal Accounts

17.1 Many members of staff may have access through their own personal accounts to social media sites such as Facebook. They are for personal use only and under no circumstances should they be used to conduct open-source internet and social media enquiries on behalf of North Norfolk District Council. This is due to the fact that it is impossible to control and the risks. As a result, it is likely to leave the Council facing liability issues over potential breaches of privacy under the HRA or other legislation such as RIPA and the GDPR.

18. Use of Mobile Phones

18.1 Work issue mobile phones should not routinely be used to carry out open-source internet and social media research within the context of this procedure. Staff should only use work mobile phones to carry out research if absolutely necessary and if used, a record must be made re the audit trail. The record should also include why it was necessary to undertake the research using a works mobile phone. Line Managers are expected to manage and oversee the use of mobiles phones being used by staff to carry out internet searches.

19. Activities by Members of the Public

19.1 If during the course of a complaint or enquiry, it is necessary to obtain internet material for intelligence or evidence from a member of the public, they may be asked to provide printed screen shots to corroborate the information. However, any subsequent internet research should be carried out by North Norfolk District Council staff and not the member of the public. This will assist with managing the activity in line with legislation and guidance. It will also reduce the risks associated with these types of enquiries. Therefore, this information should be made clear to the member of the public and documented within the relevant case notes.

20. Use of Information and Material Obtained

20.1 The material obtained from conducting open-source internet and social media research may be used as intelligence or evidence. However, it has varying levels of value due to its reliability and authenticity. The OSC have previously stated that “particular care should be taken when using data or information obtained from open or unevaluated sources such as the internet or social networks”. That is because it is not conclusive as to who

posted the information. A considerable amount of information on the internet, unless being capable of time lined is historical data. Therefore, corroboration should be sought. It is currently regarded as hearsay evidence and will require corroboration.

20.2 Unless required as evidence in criminal investigations, the material obtained should be considered as intelligence, and therefore potentially sensitive within the disclosure provisions of the Criminal Procedures Investigations Act (CPIA) in criminal cases Similar principles should apply to non RIPA. However, it is always possible that North Norfolk District Council can be ordered to disclose the information.

20.3 Any material obtained can be used during a PACE interview under caution. However, it must be recognised that it has a limited value and may call into question the authorisation procedure. It will also disclose investigation tactics which may in turn make these types of enquiries less productive in the future.

20.4 With regard to non RIPA material such as in connection with disciplinary issues there is more scope for its use due to the proceedings being civil not criminal. Seek advice if there are any doubts about whether to use the information.

21. Preservation of Evidence

21.1 Evidence obtained from the internet is digital evidence. All digital evidence is subject to the same rules and laws that apply to documentary evidence.

21.2 The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of the investigator.

21.3 It is essential to display objectivity in a court of law, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which, the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court. Therefore, it is important that evidence obtained online is preserved and presented in a manner that is able to withstand scrutiny. With this in mind, as well as the continuity and integrity of the evidence, there are recognised principles with regard to the presentation of digital evidence. These are contained within the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence, March 2012 (still current) and are:

Principle 1. No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

Principle 2. In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3. An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

21.4 These apply to North Norfolk District Council staff the same as law enforcement. With regard to principle 3, an independent third party should be able to examine those processes and achieve the same result as that presented to a court. This is likely to be the same for Civil Court.

21.5 The issue when undertaking the research is that it is not normally known at that stage whether the information will end up being used as evidence in either criminal or civil proceedings. Therefore, these procedures should be followed.

21.6 To achieve the above, the content of websites or web pages should be evidentially captured using approved video or image capture software. These provide a visible representation of how the website looked when it was visited. The created digital files will contain original source data. If such software is not available, the pages can be saved as screenshots, a standard screen capture of the viewable window or by saving the individual pages. However, this method will not produce digital evidence to the same standard. This means as well as obtaining a visual record, the code from the web pages is secured, which may become relevant to the investigation.

21.7 An audit trail should be maintained in a written log of the steps taken to reach the material obtained as evidence. 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 the General Data Protection Regulations (GDPR) data retention policy.

22. Written Activity Records

22.1 Written records known as audit trails must be recorded in **all cases** of internet research. They assist with compliance of principle 3 mentioned in section 21 earlier. They should detail all the processes applied when obtaining the information and evidence. These will need to be preserved as they may later be required for oversight and to assist with any complaints that may arise with regard to breaches of privacy, or necessity and proportionality issues. Therefore, they may be required to assist with testimony in a court or tribunal relating to the conduct of the examination and procedure adopted.

22.2 Audit Trail Contents

- Date time the research took place
- Requester ID
- Record of any approval
- Subject of the research
- Offence under investigation or other reason
- Necessity and proportionality
- Privacy issues
- Cross refence to any RIPA or non RIPA unique numbers
- If connected to a complaint etc. cross ref to any unique number attributable to the complaint
- Aim and objectives, purpose of investigation
- Sites visited

- Summary of content extracted or printed off
- Account used
- Any other relevant info

22.3 An internet research form is attached at Appendix A which can be used to record the information. This will also assist with having a separate form for disclosure provisions under CPIA.

23. Criminal procedures Investigations Act (CPIA)

23.1 The CPIA sets standards and procedures relevant to criminal investigations. It provides the guidance to all staff involved within an investigation as to their responsibilities. This guidance is designed to:

- Regulate the investigation process
- Regulate the recording and retention of material that is found or is generated in the course of an investigation
- Regulate what is disclosed to the prosecutor and the defence
- Ensure that the investigation is fair
- Stipulates retention time frames for the material obtained

23.2 All research in connection with a criminal investigation must be documented and retained in line with CPIA.

23.3 The CPIA Codes of Practice can be obtained from:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf

24. Training

24.1 A risk assessment approach will be required to identify the level of training and the staff to be trained which assists with compliance with principal 2 mentioned at 20.1 earler. Departmental line managers will have the responsibility of assessing the training requirement. However, this should be linked to the overall corporate strategy with regard to open-source internet and social media research.

25. Monitoring and Review of Procedure

25.1 This procedure will monitored an reviewed where necessary by the SRO. The minimum of an annual review will take place.

26. Further Reading

- RIPA Codes of Practice for Directed Surveillance and CHIS
- Criminal Procedures Investigations Act Codes of Practice
- Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence, March 2012
- ~~OSC procedures and Guidance 2016~~
- RIPA Directed Surveillance and CHIS Codes of Practice August 18
- General Data Protection Regulations (GDPR)

Internet Research Form

Ref no:	Department:	Date:
Subject of the research (if known) Name DOB or age Address		
Offence/incident or reason for the research:		
Why it is necessary to undertake these particular enquiries in this way:		

Privacy issues: *Detail any privacy issues identified to date- how you will manage any private information obtained as a result of the research, including it's storage and use:*
Authorised By

This log is to record the research undertaken and must include all sites visited and contain rationale for continuing the research taking into account necessity, privacy issues identifies and proportionality.

Internet Research Activity Log		
Date	**Activity undertaken including sites visited**	**By whom**