Northamptonshire Police

If printed, copied or otherwise transferred from the Policies and Procedures Intranet/Internet Site this document must be considered to be an uncontrolled copy. Policy amendments may occur at any time and you should consult the Policies and Procedures Intranet/Internet Site if in doubt.

Open Source Research and Online Investigation

Reference Number		Version	12/17
Department Responsible	Digital Intelligence Unit		
Author	[redacted]		
Senior Owner	DI 654 Andrew Tuff		
Effective Date	06/12/2017	GSC Marking	Official
Type	Policy		

1. Introduction

1.1 The use of the internet and social media is constantly evolving and means best practice will constantly evolve too. This policy establishes corporate standards that will ensure all online research and investigations are conducted lawfully and ethically by Northamptonshire Police.

1.2 There is an increasing demand on Law Enforcement to investigate and identify data that is stored in locations accessed via the internet. There is also a public expectation that the internet will be subject to routine "patrol" by law enforcement agencies. It is recognised that this research can be a creative intelligence tool to be used to find information on people of interest and to generate valuable intelligence and evidence.

1.3 Patterns of criminal planning are changing to embrace technological advances. Social media and private electronic communications provide greater anonymity for offenders and enable their activities to proceed on a global scale.

1.4 Any investigation or intelligence gathering conducted using the internet must be done in accordance with our legal obligations and in a manner that does not place the Force at risk of legal challenge or jeopardise any ongoing or future investigation and law enforcement activity. This guidance will ensure we meet these requirements whilst still maintaining a useful avenue for investigation.

2. Legislative Compliance

2.1 The deployment of open source tactics will have a significant impact on a number of rights under ECHR and the Human Rights Act. This policy has therefore been drafted in order to comply with that legislation together with the following:

- Freedom of Information Act;
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Computer Misuse Act 1980 (CMA)
- Data Protection Act 1998 (DPA)
- Criminal Procedure and Investigations Act 1996 (CPIA)
- Police Act 1997
- Management of Police Information 2010 (MOPI)
- CESG(The National Technical Authority for Information Assurance – Good Practice Guide Online Social Networking
- NPCC Data Communications Group – Researching and Targeting Social Networks for Evidence or Intelligence (This is based around College of Policing advice)
- NPCC – Good Practice Guide for Computer Based Electronic Evidence
- Investigatory Powers Act 2016

3. Policy Statement

3.1 Northamptonshire Police will ensure that any open source activity carried out is done so in a manner that does not compromise any current or future investigation or the tactics currently available. The Force will ensure that evidence obtained online is preserved and presented in a manner that is able to withstand scrutiny in any subsequent criminal proceedings.

4. Monitoring and review

4.1 The senior owner will review the content of this guidance annually to ensure that this is relevant and up to date. The author has agreed that this document will be reviewed within 12 months of the effective date.

5. Force Impact

5.1 The implementation of this policy will demonstrate to the public, victims, partners and a range of national law enforcement agencies that Northamptonshire intends to develop and implement a strategy that will ensure an effective and efficient tactical response that will raise public confidence in relation to the local investigation of any crime with a Cyber Digital element.

6. Background Information

6.1 Open source research is the collection, evaluation and analysis of material from online sources available to the public, whether on payment or otherwise, to use as intelligence or evidence within a criminal investigation.

6.2 NPCC provides the following definition which may assist those involved in online research and investigation:

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

6.3 For the purposes of this policy, it is recognised that commercial subscription databases may contain some data not available to the public but within the terms of the policy they are still considered open source.

6.4 The searching, retrieval and use of information from the internet must be carried out in a manner which is compatible with the Human Rights Act, in particular Article 8 (Respect for Family and Private Life) and Article 10 (Freedom of Expression). Any interference with these rights must be necessary, proportionate and justified.

6.5 It is essential to consider the effect any collateral intrusion on the private and family life of other people not directly connected with the subject/s of the investigation.

6.6 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 instances, the individual carrying out that activity.

6.7 Staff engaged in research or investigation over the internet must take precautions to protect the security of themselves and police computer systems.

7. Regulation of Investigatory Powers Act (RIPA)

7.1 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.

7.2 The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the Social Network being used works. Researchers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

8. Directed Surveillance Authorities (DSAs)

8.1 It must be borne in mind that repeat viewing of open source sites may constitute directed surveillance. This must be assessed on a case by case basis. Viewing restricted information, that which is not publically available, covertly online will generally constitute surveillance. It is likely that private information will be obtained, therefore a DSA must be sought. Private information will include information on social networking sites that has privacy settings applied.

8.2 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as open source or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example).

8.3 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.

8.4 This will include the situation where a 'friend request' is made and accepted, as the user will then be able to see private information about the subject and their 'friends'; information that is not publicly available.

8.5 Joining a group may not provide access to private information about individuals, therefore a DSA will not necessarily be required. This will, however, depend on the nature of the group and the information likely to be obtained, advice can be sought from the Central Authorities Bureau.

8.6 When login details obtained for an account (such as email, social media etc) along with written consent from the account holder, a DSA will be required to view the private accounts of the user's other 'friends' unless consent is obtained from all parties whose information may be viewed.

8.7 If focussed on a specific individual or group, systematic trawling and analysis of recorded data, or consistent monitoring of it, may amount to surveillance. A DSA must therefore be considered.

8.8 During the course of an investigation the nature of the online activity may evolve. Staff must continually assess and review their activity to ensure it remains lawful and compliant with RIPA.

8.9 National guidance states that sending a 'friend request' or joining a group, is unlikely to constitute establishing or maintaining a relationship as the request can be accepted or denied without challenge. This is unlikely to require a CHIS authority. It may however require a Directed Surveillance Authority (DSA). **It is Northamptonshire Police policy that only staff in the Digital Intelligence Unit will send 'friend requests'.**

9. Covert Human Intelligence Source (CHIS)

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

- they covertly use such a relationship to obtain information or to provide access to any information to another person; or

- they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

9.2 Support around this area of activity will be provided by EMSOU Covert Unit and their advice must be sought at the earliest opportunity.

9.3 Authorisation as a CHIS need only be sought when it is anticipated that the relationship will be developed beyond this initial contact.

10. Security

10.1 Security is everyone's responsibility and this remains true when working on the internet. The use of the internet is monitored and will be subject to a high degree of scrutiny.

11. Open Source Authorisation and Levels of access

11.1 The NPCC agreed framework will form the basis for all lawful online activity and must be complied with. These 5 levels have been approved nationally to define the levels of activity for Open Source Intelligence/research (OSIR) and Covert Internet Investigation (Undercover officer on line)

11.2 Levels 1 - 3 are open source investigation/research; levels 4 & 5 are specialist activity on the internet which requires specific authority and specialist training and are not considered open source investigation.

11.3 The criteria detailed in the following standards will be seen as a minimum to carry out operational activity on the Internet. Departments will assess their operational requirements individually and set operational criteria with input from the Digital Intelligence Unit.

12. Level 1 - Overt (i.e identifiable as Law Enforcement) Open Source Research & Social Media Engagement

12.1 This level of access is available for all Northamptonshire Police employees.

12.2 Authority and Approval

No level of authority is required, but must adhere to force policy regarding use of Computers. The investigation/research activity is considered overt. Research is permissible on publicly accessible search areas of the internet such as map viewing, street views, local authority sites, auction sites or any publicly available website which has no requirement to register details to gain access.

12.3 Evidential Capture

This requires the researcher to clearly show where the intelligence or product has been gathered from. The time; date and Unique Reference Location (URL) are to be documented along with a screen shot or download of any video or image by using the software provided. This then needs to be stored in a suitable location for any future requirement or court processes. Advice can be sought from the Digital Intelligence Unit.

12.4 Computer type to be used

These enquiries may be conducted using a standard Force desktop/PNN networked computer.

12.5 Training

There is no requirement for specialist training for this level of access.

NCALT e-learning packages are available to assist in understanding of the issues involved.

- MoPI Levels 1 - 4
- Communications Data in Investigations
- Introduction to Communications Data
- Cybercrime
- MCCT

12.6 Use

This level may only be used where you can be certain it would not affect your investigation if the person or site being visited knew the police were looking at their information. This may be used for research across publicly accessible search areas of the

Internet such as map viewing, street views, local authority sites, auction sites or any publicly available website provided there is no requirement to register details/create an account to gain access. As the investigation/research activity is considered overt, there is not usually a requirement for any RIPA or Police Act Authority.

If you are required to log on or create an account this must be approached using level 2, 3.

Examples of how level 1 may be used:

- To research a name on Social networking sites;
- Check for phone numbers or identify a known number prior to subscriber requests;
- View Public Profiles or Groups;
- Generic search for missing people;
- Search Google / eBay

12.7 Level 1 - Important Note

This is to be used for searching only. It must not be used where you are required to create a log on account or otherwise register to access the information. You must not use your own/home/personal account to access information or services for investigation purposes. Every enquiry leaves a footprint that can be traced. Individuals have in the past been identified as Police Officers and their home address located.

13. Level 2 - Covert Basic Open Source Research

13.1 Authority and Approval

- Northamptonshire Police will comply with the current NPCC advice and will be cognisant of the view from the Office of The Surveillance Commissioners (OSC).

- It is expected that if this activity is anything more than an initial view and in fact is part of a specific operation or investigation than a DSA will be in place. Advice will be provided by the Central Authorities Bureau.

13.2 Evidential Capture

This requires the researcher to clearly show where the intelligence or product has been gathered from. The time; date and Unique Reference Location (URL) are to be documented along with a screen shot or download of any video/image by using the software provided. This then needs to be stored in a suitable location for any future requirement or court processes. Advice can be sought from the Digital Intelligence Unit.

13.3 Computer type to be used

Any investigation or research at this level must be conducted on non-attributable (traceable) computer systems.

13.4 Training

This level of enquiry may only be undertaken by authorised staff (i.e. those who have successfully completed a recognised Level 2 open source course).

13.5 Use

This level of access is used where it is required to log into/create accounts for accessing and searching sites or services. On-line False Identities (OFI) can be used to log onto Social Networking sites.

A record of all the processes applied to the Open Source Research must be created and preserved. A practitioner may need to testify in court not only in relation to the conduct of the examination, but also the validity of the procedure.

- Level 2 trained researchers can capture evidence.
- All activity conducted online must be completed to an evidential standard with still image and video capture. Due to the ever changing and volatile nature of online material it may not be possible to replicate or view the same material again. Material must be captured and then can be assessed as per CPIA rules or PII procedure.
- Relevant intelligence will be evaluated and submitted into the Niche Intelligence System.
- Those trained at Level 2 are not permitted to perform account takeovers.
- It is Northamptonshire Police policy that staff trained to Level 2 will have no interaction - no befriending subjects, following, posting on timelines or joining groups.

14. Level 3 Covert Advanced Open Source Research

14.1 Authority and Approval

The same levels of authority and approval are required as outlined in Level 2, however, in relation to closed groups, forums and social networking sites, a DSA must be considered and in the majority of cases will be required. It is expected that if this activity is anything more than an initial view and in fact is part of a specific operation or investigation than a DSA will be in place.

By their very nature chat rooms and online forums are sites which promote communication and the formation of relationships. Extreme care must be taken when entering these environments as the threshold for either a DSA or CHIS authority could easily be met. A closed forum is considered to be an online message board which requires a user to authenticate themselves via a username and password before full unobstructed access is granted. It must be noted that many closed forums provide limited public access and the information sought may be obtainable from the non-restricted content without the need for joining.

Directed surveillance authorities do not necessarily authorise an officer to register with a closed site and there is a very real danger that registration WILL involve the formation of a relationship with the site administrator and this will require additional authorities (Intrusive surveillance, CHIS or CII). Unfortunately the officer will not know whether or not registration is automated until they have embarked on that process, at which time it is too late.

In order to mitigate the occurrences of this staff will task the Digital Intelligence Unit to carry out an initial reconnaissance against closed forums of interest. They will establish whether or not authority to join is automated or requires human intervention, the number of registered forum members and the level of activity within the forum. Once this information is obtained staff will be in a position to make an appropriate risk assessment in relation to requiring a DSA; authorising entry to the forum for the purposes of monitoring the group in question. If entry is not possible then further CHIS or UCO tasking will be considered.

14.2 Evidential Capture

This requires the researcher to clearly show where the intelligence or product has been gathered from. The time; date and Unique Reference Location (URL) are to be documented along with a screen shot or download of any video/image by using the software provided. This then needs to be stored in a suitable location for any future requirement or court processes. Advice can be sought from the Digital Intelligence Unit.

14.3 Computer type to be used

Any investigation or research at this level must be conducted on non-attributable (traceable) computer systems.

14.4 Training

Staff conducting these enquiries must have received Advanced Open Source Training to ensure they investigate and research using the internet to produce consistent and quality results. Users will have been trained to conduct open source research either internally or through an approved external course. A list of those officers will be maintained.

14.5 Use

Researchers are trained to an advanced level. They use advanced open source intelligence gathering techniques and generally conduct research under a Directed Surveillance Authority if required.

At this level researchers will gain access to both open and closed online portals and conduct in depth profiling of individuals online presence, in accordance with the limitations of the relevant DSA.

Researchers will be allowed to use accounts and search using them. On-line False Identities (OFI) will be used to log onto Social Networking sites. **OFI's are issued and registered by the Digital Intelligence Unit.**

15. Level 4 - Internet and Technical Investigation

15.1 Any activity around Technical Investigations or any specialist activity that may fall under the definition of 'Equipment Interference' requires consultation with the Digital Intelligence Unit. Tactics and techniques involved require advanced levels of training.

16. Level 5 – Covert Internet Investigation (CII)

16.1 This level of access is required where it is proposed to interact with online groups or individuals. This level of enquiry may only be undertaken by specially trained staff. Advice must be sought from the EMSOU Covert Unit at the earliest opportunity.

17. Operational Risks (Traces)

17.1 Any activity carried out over the internet leaves a trace or footprint which can identify the device used and, in some instances, the individual carrying out that activity. Persons engaged in investigation and research over the internet must take precautions to protect the security of themselves and of police computer systems.

17.2 Internet Service Providers (ISP) maintain a record of IP addresses and the sites visited. Websites may record IP addresses as well as other details about the computer used including the browser, operating system, computer name etc. Records are often kept of the time and date of each visit, in addition to the sites the visitor came from and went to. Websites can install cookies on to a computer in order to identify the user, should they return to that site.

18. Intelligence Submissions

18.1 If we increase our capability we will increase our intelligence output. There is little purpose conducting open source research if we do not create a wealth of intelligence that can be shared.

18.2 All intelligence submissions will be submitted in line with Niche input standards and drafted in line with National standards. For example the identification of any phone numbers must be referenced by the relevant URL to ensure any other party is able to retrieve that information. The source will be recorded as the particular application or forum showing the intelligence and the log text will contain the specific link e.g. http://1234ABC/general/defg5678.com

19. On-Line False Identities (OFI)

19.1 An OFI is defined as any on-line user account that does not identify the user as being a Police employee. The Digital Hub / DMI manager retains oversight of all OFI's.

19.2 The Digital Intelligence Unit will maintain a register of every OFI created and in use by any member of staff and will be subject to review. This central record will also be open to inspection by the Office of Surveillance Commissioners.

19.3 OFI's will only be created by the Digital Intelligence Unit.

19.4 Online False Identities are recognised covert assets and as such require strict management around their use and deployment. Only those officers trained in the use of Open Source Research Techniques will have access to an OFI.

19.5 The OFI will be individual to each officer and is only to be used by them. It is not permitted to allow other persons access to and use of the OFI. Each officer is responsible for the maintaining and storage of records created during the use of each OFI deployment. These will be made available for audit purposes and review on request.

19.6 Any changes to passwords and security options for each OFI will only be made with agreement and oversight of the Digital Intelligence Unit.

19.7 On Line False Identity types –

- 'Grey' – This is an online identity that facilitates the 'key in the door' to create a log in for accounts and services. The 'Grey' does not have any imagery or profile information other than the minimum required to create the account.

- 'Developed' – Online identities of this type may have a backstory to the profile. This may include profile imagery, likes, follows and timeline updates. **Northants Police Policy around the use of OFI is that only officers and staff in the Digital Intelligence Unit will have access to 'Developed' identities.**

- 'Enhanced' – These are online identities that maintain their covert legend[s] and cover stories and as such will need to behave and act on line as expected by others. This will require interaction with people other than authorised subjects, such as accepting friend requests or invites to groups. **Northants Police Policy around the use of OFI is that only officers and staff in the Digital Intelligence Unit will have access to 'Enhanced' identities.**

19.8 The use of OFI's is just one tactic in our covert ability to prevent and detect crime or prevent disorder. Other alternative and less intrusive methods must be considered at all times.

19.9 All activity obtained through the use of an OFI will be recorded using audio visual software or contemporaneous logs. This in accordance with the standards expected for Advance Open Source Research. Any investigation or research with the OFI must be conducted on non-attributable computer systems in accordance with Open Source Research guidance and procedure.

19.10 All applications for an OFI must be made to the Digital Intelligence Unit who will consider the operational necessity and make the appropriate arrangements.

20. Compromise procedure

20.1 If the use of an OFI or Open Source Research is compromised in any way then the following procedure will be adopted:

- Immediately withdraw from the site

- Immediately notify the Digital Intelligence Unit supervisor of the nature of the compromise and the OFI used to gain access

- Document an account of the events

- Suspend the use of the OFI

- On notification of a compromise the Digital Intelligence Unit will undertake review and de-confliction within other covert assets

- Any activity considered to be in breach of force standards and policy will reported to PSD.

21. Open source data transfer process

21.1 The purpose of this process is to ensure information recovered from the Internet using Non Attributable Open Source equipment is transferred to Force systems in a safe and secure manner. This will prevent unnecessary risk occurring to Force systems from viruses or malware which can unknowingly be captured from the internet during legitimate Police activity.

21.2 This process is applicable to all Officers and members of staff who have access to Non-attributable equipment and are appropriately trained in Open Source Research and Investigation.

21.3 Users will place all files and data required to be transferred to Force systems on an approved USB device. Once connected to a Force Networked machine installed WAVE protection will scan the USB device and its content. Once complete the files can be placed in the relevant depository required by the user. Microsoft Endpoint Protection works as an additional measure to re-scan files for virus/malware as soon as any transfer occurs either to or from the USB device.