35201 PROCEDURE – OPEN SOURCE INVESTIGATION AND RESEARCH

Version	1	Last updated	08/01/2019	Review date	08/01/2020
Equality Impact Assessment			Low		
Owning department			Intelligence		

1. About this policy

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

1.2. Open source research and investigation is a powerful tool against crime. Hampshire Constabulary needs to ensure that any collection of information from the internet for a policing purpose is conducted in such a way that:

- The integrity of any evidence gained is maintained;
- Officers and staff consider whether their evidence or intelligence gathering is likely to interfere with a person's right to respect for their family life (Human Rights Act 1998 - Article 8) and, if so obtain appropriate authorisation under the Regulation of Investigatory Powers Act 2000 for their research or specialist assistance.

1.3. The following are not compromised:

- The hardware/software infrastructure of police computer systems;
- Police tactics;
- Ongoing and future police operations;
- The personal safety of individuals; and
- The reputation of the organisation.

2. General principles

2.1. Online communication via the internet has become the preferred method of communication between individuals, within social groups or indeed with anyone in the world with internet access.

2.2. Such communication may involve web sites, social networks (e.g. Facebook), chat rooms, information networks (e.g. twitter) and/or web based electronic mail.

2.3. 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.

2.4. Online research and investigative techniques capable of interfering with a person's Article 8 rights should be used only when necessary and proportionate.

2.5. Regulation of Investigatory Powers Act (RIPA), the Data Protection Act (DPA) and the Government Data Protection Regulations (GDPR) 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).

2.6. The Home Office Covert Surveillance Code of Practice also provide statutory guidance on the use of some of these techniques (see paragraph 2.9 below).

2.7. 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.

2.8. Public authorities must ensure that any interference with this right is:

a) Necessary for a specific and legitimate objective – such as preventing or detecting crime;
b) Proportionate to the objective in question;
c) In accordance with the law.

2.9. The Covert Surveillance and Property Interference Code of Practice (August 2018) provides clear guidance, paragraph 3.15 states that:-

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 a 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.

Further guidance can be found in paragraphs 3.10 to 3.17 HERE.

3. Procedure

3.1. Purpose of procedure

3.1.1. This procedure is intended to assist officers and staff in acting within the law, determining whether such authorisation is appropriate and using the appropriate tools to achieve their operational objectives.

3.1.2. The training that is required for staff to be able to carry out activity relevant to the 5 levels of Open Source Investigation and Research is set out in section 4.

3.2. Operational Risk

3.2.1. Any online research and investigation leaves a trace or 'footprint'.

3.2.2. An early decision must be made as to whether it is necessary to ensure that research or investigation is non-attributable (covert). This means that it cannot be traced back to law enforcement or to identifiable individuals.

3.2.3. Any research or investigation will otherwise have the potential to be attributable or capable of being traced to law enforcement.

3.2.4. The SPECTRUM network allows for covert open source research to be conducted on a centrally managed environment which is safe and secure (at NPCC level 2). The network is fully auditable by Police National Systems Office Integrity Auditors and an overview is maintained by the Force Operational Security Advisor.

3.2.5. Carrying out attributable activity to Law Enforcement (e.g. by use of title, PNN email address) the SPECTRUM network presents a risk of compromise to the equipment and investigations and must therefore never occur.

3.3. Health and Safety

3.3.1. Staff engaged in Open Source Investigation and Research will inevitably spend periods of time working form desks and should therefore should adhere to advice provided by Occupational Health and Wellbeing such as the back care information contained on the force Intranet pages.

4. NPCC Five Levels of Open Source Investigation & Research (OSIR)

4.1. The National Police Chief's Council sets 5 levels of open source investigation and research. Activity at Level 5 (UC online) will not be carried out by Hampshire staff or officers but assistance can be sought through the CCU, CAB and SEROCU in respect of this activity where required.

4.2. The five levels can be summed up as (further detail below):

- Level 1 – Overt open source research.
- Level 2 – Covert, non-repeated open source research.

- Level 3 – Covert advanced open source research and monitoring of targeted individuals (RIPA DSA requirement).

- Level 4 – Covert advanced open source research of groups and network (without establishing or maintaining a relationship) for the purpose of facilitating the covert investigation or monitoring of targeted individuals (RIPA DSA requirement).

- Level 5 – Undercover Online activity (RIPA CHIS authority requirement).

4.3.

Level	One - Overt OSIR
Purpose	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 which has no requirement to register details to gain access.
Authority	As the investigation/research activity is considered overt there may not be a requirement for any RIPA authority. However, investigators need to consider - each time a repeat enquiry is made, the proportionality, necessity and lawfulness of the enquiries must be considered and advice sought from the Central Authorities Bureau as it is likely that a RIPA authority would be required.
Rules	Must adhere to Force procedure& procedure – '22207 Procedure - Internet Web Browsing'.
Training	Staff conducting this activity will have received level 1 training (NCALT Cyber Crime and Digital Policing – Introduction).
Computer	Can be conducted using any Hampshire Constabulary internet enabled standard network computer (which excludes the "SPECTRUM" terminals) provided there are no concerns about the police leaving a digital footprint.
Notes	• You should consider the impact of the subject identifying that police are viewing open source information on them and how this may impact on the investigation, revealing tactics and available evidence. • the facility exists for officers to use the HantsPol Enquiries Facebook account for overt, non-repeated research
Further advice	Digital Media Investigator (DMI); Central Authorities Bureau (CAB); Open Source Intranet pages.

4.4.

Level	Two – Core OSIR
Purpose	For intelligence, investigation/research across publicly accessible search areas of the internet where the fact of the research is intended to remain unknown to/by the subject, including through the use of a false persona.

	This can be: • staff conducting more in-depth open source investigation or research to assist their investigations; or • Searches across whole of internet using tools such as search engines, people search sites, social network sites and voice over internet protocol (VOIP).
Authority	**On each and every occasion active consideration must be given to the need for a DSA under RIPA – please see paragraph 2.9 above and paragraphs 3.10 to 3.17** HERE. The use of a False Persona be authorised in writing by your supervisor and its creation authorised by the Police National Systems Office. Passive False Persona profiles can be used to log into social networking sites but there must be no interaction – no befriending subjects, poking, writing on walls or joining groups.
Rules	There must be no activity which would require interaction with another party.
Training	Staff conducting this activity must have received MCCT Level 2 training as a minimum.
Computer	This activity must only be carried out on SPECTRUM terminals provided by Hampshire Constabulary for this activity. These devices must not be used for any other overt activity (or any personal use).
Notes	Product recovered must be evaluated and submitted into Force intelligence management system in most cases using an Intelligence Report.
Further advice	Digital Media Investigator; Central Authorities Bureau (CAB) Force Operational Security Officer (FOSA) Open Source Intranet pages.

4.5.

Level	**Three – Covert Advanced OSIR**
Purpose	Covert advanced open source intelligence investigation, research and monitoring. This monitoring is highly likely to amount to surveillance and therefore require a RIPA authority.
Authority	**On each and every occasion active consideration must be given to the need for a DSA under RIPA – please see paragraph 2.9 above.** Engage with the CAB for advice before commencing this type of activity. The use of a False Persona be authorised in writing by your supervisor and its creation authorised by the PNSO.

	Passive False persona profiles can be used to log into social networking sites but there must be no interaction – no befriending subjects, poking, writing on walls or joining groups.
Rules	There must be no activity which would require interaction with another party.
Training	Recognised advanced open source training including relevant legislation and case law.
Computer	This activity must only be carried out on dedicated standalone covert computer devices provided by Hampshire Constabulary for this activity. These devices must not be used for any other overt activity (or any personal use).
Notes	Product recovered must be evaluated and submitted into the Force intelligence management system in most cases using an Intelligence Report.
Further advice	Digital Media Investigator; Central Authorities Bureau; Open Source Intranet pages.

4.6.

Level	**Four - Covert internet and network investigations**
Purpose	Covert internet and network investigations.
Authority	A Directed Surveillance RIPA authority will be required where repeated monitoring of a subject(s) takes place.
Rules	At this level, trained officers may send ‘friend’ requests if appropriately authorised. Further contact is not permitted. Hampshire has no L4 trained officers South East Regional Organised Crime Unit (SEROCU) resources can be requested to assist with this activity via Force tasking processes.
Training	Recognised advanced open source training including relevant legislation and case law.
Computer	This activity must only be carried out on SPECTRUM terminals provided by Hampshire Constabulary for this activity. These devices must not be used for any other overt activity (or any personal use).
Further advice	Central Authorities Bureau; SEROCU; Open Source Intranet pages.

4.7.

Level	Five - Undercover officer online, Covert Internet Investigator
Purpose	Undercover officer online, covert internet investigation.
Authority	Will require CHIS authorisation under RIPA from an accredited Authorising Officers (seek advice from CAB).
Rules	Hampshire has no L5 trained officers and therefore officers and staff must not engage in this activity. SEROCU resources can be secured via Force tasking processes.
Training	Undercover Officer Online course or equivalent.
Computer	As determined by the South East Covert Operations Unit.
Notes	Product recovered must be evaluated and submitted into Force intelligence management systems in most cases using an Intelligence Report.
Further advice	Central Authorities Bureau; SEROCU; Open Source Intranet pages.

5. Online False Personas

5.1. Trained Investigators are allowed to create 'false personas' to allow covert investigations to be carried out with a reduced risk of detection or compromise, subject to compliance with force policy 35200 and this procedure. It is essential that when we conduct online investigations we adhere to all relevant legislation, in particular RIPA, the Data Protection Act, GDPR and ECHR.

5.2. To create a false persona you MUST have completed at a minimum, the Mainstream Cybercrime Course.

5.3. You must get authority in writing from the Police National Systems Office to create a False Persona.

5.4. You must register that false persona with the Police National Systems Office.

5.5. You must NEVER allow anyone else to use a false persona you have created or registered in your name.

5.6. Use of a False Persona in any investigation must be authorised in writing prior to its use by your line supervisor who is responsible for the day to day supervision, to be satisfied that its use is authorised and lawful.

5.7. Use of the False Persona must be recorded locally and an audit can be undertaken by the PNSO and FOSA via SPECTRUM or spot checks.

5.8. Use of False Personas will be subject of auditing to ensure compliance.

5.9. Hampshire Constabulary staff and officers are not permitted to covertly interact, establish or maintain any form of relationship with subjects (Level 4 & 5 activity) whilst carrying OSIR enquiries.

6. Roles and Responsibilities

6.1.

Open Source/ False Persona User 1. Engaging with Continuous Professional Development opportunities to maintain skills in respect of this activity. 2. Remaining up to date on policy, relevant IPCO guidance and legislation governing the use of Open Source research and False Personas. 3. Record keeping of all False Persona use and reporting use to the Police National Systems Office in accordance with section 5 of this Procedure. 4. Obtaining authority from a supervisor to use a False Persona as part of an investigation on each occasion that its use is considered necessary and proportionate for the objectives.
Local Supervisors 1. Ensuring staff who are trained Open Source and False Persona users have sufficient time for CPD. 2. Remaining up to date on policy, relevant IPCO guidance and legislation governing the use of Open Source research and False Personas. 3. Consider whether a 'User's' request to use a False Persona within an investigation necessary, proportionate and lawful.
Central Authorities Bureau 1. Assist in the maintenance and implementation of current force guidance 2. Coordination and promotion of "what works well" and "not so well" via DII group. 3. Identifying and promoting changes in legislation and IPCO guidance 4. Compliance with legislation through the review of potential breaches escalated by Police National Systems Office (PNSO) and the Force Operational Security Advisor (FOSA). 5. Flagging relevant Directed Surveillance Authorities to FOSA to assist in his role.
Police National Systems Office 1. Verifying that a User is authorised to use false personas. 2. Maintaining central register of those authorised and trained to use a false persona. 3. Audit of the SPECTRUM system to ensure compliance. 4. Responsible for cancelling authority to use false personas (no use in 3 months – unless specific CPD is carried out). 5. Identify mission creep and potential breaches of RIPA escalating to the CAB and FOSA where necessary. 6. Provide a link to Learning and Development regarding policy and procedure, newly trained staff, CPD and refresher training.

7. Support the FOSA with systems audit.
Force Operation Security Advisor 1. Visiting trained staff, viewing their records and accounts to: i) Check compliance with guidance, force policy, procedure and legislation (e.g. mission creep) ii) Reduce risk to covert operations (e.g. cross pollination, excessive use of profiles) iii) Promote “what works well” and “not so well” iv) Enhance knowledge of staff / supervisors
Covert Intelligence DCI 1. Provide strategic responsibility for the implementation of this procedure.

7. Implications of Procedure

7.1. Legal

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

a) Human Rights Act 1998 / European Convention on Human Rights

b) Regulation of Investigatory Powers Act 2000

I. Part I – Interception of Communications and the Acquisition of Communications Data

II. Part II – Surveillance and Covert Human Intelligence Sources

a) Police Act 1997 Part III

b) Computer Misuse Act 1990

c) Data Protection Act 1998

d) Government Data Protection Regulation 2018

7.2. Risks

7.2.1. Improper use of the internet for research and investigation presents risks to staff, operations and investigations and legal and reputational risk to the Force.

7.2.2. All activity should take place according to the policy and related procedure and where necessary the advice of a Digital Media Investigator or the Central Authorities Bureau should be obtained.

7.2.3. Hampshire Constabulary reserves the right to monitor and / or audit the use of its equipment to ensure compliance with force policies, standards and legislation.

7.3. Consultation

7.3.1. This procedure has been created in consultation with the Force lead for Digital Investigation and Intelligence (ACC Crime and Criminal Justice), the Force Authorising Officer (AO), the Covert Investigation Support Unit (CISU), and relevant users.

8. Monitoring and evaluation

8.1. This procedure will be owned by the ACC Crime and Criminal Justice, it will be reviewed and monitored by the Digital Investigation and Intelligence Group.

9. Review

9.1. The procedure will be reviewed following relevant changes to legislation, Authorised Professional Practice (APP) and any change to roles and responsibilities within Hampshire Constabulary.

9.2. An annual review will also take place.

10. Other related policies, procedures and information sources

10.1. Related policies

10.1.1. Media

10.1.2. Social Media

10.1.3. Authorisation-RIPA

10.1.4. Covert Human Intelligence Sources

10.1.5. Professional Standards

10.2. Related procedures

10.2.1. Non-Attributable (Covert) Internet Equipment- Specification and Use.

10.2.2. The Capture, Recording, Storage and Retention of Digital Investigation and Intelligence Material

10.3. Information sources

10.3.1. RIPA Codes of Practice

10.3.2. AD203 Equality Impact Assessment

Origin: Intelligence