National Offender
Management Service

National Security Framework Ref: NSF 4.5a

INTELLIGENCE – REGULATION OF INVESTIGATORY POWERS ACT
Open Source Research on the Internet and social networking sites

This instruction applies to :-		**Reference :-**
Prisons NOMS HQ		**PSI 27/2015** **AI 17/2015**
Issue Date	**Effective Date**	**Expiry Date**
5 August 2015	5 August 2015	4 August 2019
Issued on the authority of	NOMS Agency Management Board	
For action by	All staff responsible for the development and publication of policy and instructions ☒ NOMS HQ ☐ NOMS Immigration Removal Centres (IRCs) ☒ Public Sector Prisons ☒ Contracted Prisons***** ☒ Governors ☒ Heads of Groups ☒Regional and Local Corruption Prevention Managers ☒ Establishment Functional Head of Security/Operations ****If this box is marked, then in this document the term Governor also applies to Directors of Contracted Prisons***	
Instruction type	***service specification support/service improvement/legal compliance***	
For information	All staff in prisons and HQ	
Provide a summary of the policy aim and the reason for its development/revision	This PSI sets out the arrangements and restrictions for gathering personal information from the Internet for intelligence or investigative purposes.	
Contact	Security Group : CAB E-mail : spoc@noms.gsi.gov.uk CAB hotline : 0300 047 6354 Policy : 0300 047 6171 E-mail : barney.clifford@noms.gsi.gov.uk	
Associated documents	Acquisition of Communications Data Code of Practice Covert Surveillance and CHIS Codes of Practice PSI 49/2011 – Prisoner Communications Services PSI 22/2012 – Covert Surveillance PSI 23/2012 – Regulation of Investigatory powers act Covert Human Intelligence Sources PSI 24/2014 – Information Assurance Policy PSI 25/2014 – IT Security Policy PSO 1300 Investigations PSO 1215 Professional Standards: Preventing and Handling Staff Wrongdoing	

	PSI 06/2010 Conduct and Discipline PSI 28//2013 NOMS Outside Activities Related Service Specification Related Operating Models Related Direct Service Costs and Assumptions paper Related Cost Spreadsheets See: http://www.justice.gov.uk/about/directory-services.htm
Replaces the following documents which are hereby cancelled: - None	
Audit/monitoring: -Monitoring of compliance will take place through the operational line.The arrangements are subject to inspection by inspectors of the Interception of Communications Commissioners Office (IOCCO) and the Office of Surveillance Commissioners (OSC)	
Introduces amendments to the following documents: -None	
Notes: ***All Mandatory Actions throughout this instruction are in italics and must be strictly adhered to.***	

CONTENTS

Hold down “Ctrl” and click on section titles below to follow link

1. Executive Summary

Background

1.1 Open source research is the name given to law enforcement and public authorities' capacity to view, collect, process, and analyse publicly available personal information stored on the Internet. This information can be invaluable for Managers when assessing whether intelligence or allegations have any substance and require further investigation. Quite often, open source research is the least intrusive and essential first step in an intelligence gathering investigation and can either prove or refute allegations at the outset.

1.2 It is necessary for NOMS to carry out investigations to, amongst other things, prevent and detect crime, to maintain security and control, on the grounds of protecting the public, or with regard to corruption or disciplinary matters.

1.3 The Human Rights Act (HRA) 1998 incorporated into UK law the rights set out in the European Convention on Human Rights (ECHR). One such right is the right to respect for private and family life (Article 8). Where NOMS seeks to obtain private information by means of covert investigative techniques it is likely that that this right will be engaged. The authorisation procedures in the Regulation of Investigatory Powers Act (RIPA) are designed to ensure that any interference with this right is likely to be justifiable as being in accordance with the law, necessary in pursuit of a legitimate aim, and proportionate.

1.4 NOMS has powers under RIPA to carry out covert surveillance operations and manage Covert Human Intelligence Sources (CHIS) under part 2 of RIPA and able acquire communications data under part 1 of RIPA. The interception of communications is made lawful by Section 4 (4) of RIPA, where it is activity undertaken in accordance with powers in the Prison Rules. There will be times that open source research may engage RIPA powers and therefore appropriate authorities must be sought.

1.5 *There are also obligations to manage intelligence and material gathered for investigative purposes under the Data Protection Act (DPA) and data protection principles – all personal data must be managed in accordance with that Act and those principles.*

1.6 This PSI then sets out what is allowed in terms of online investigations, who can carry them out, and where additional powers should be sought under RIPA. There is a restricted PSI, which contains greater detail and tradecraft for managers and investigators.

1.7 Since 2011, all open source applications have been made to the National Intelligence Unit (NIU) and the research and in some cases associated action has all been carried out centrally. This has been on the basis of cost and in order to ensure that information is captured in evidential format correctly. This PSI allows appropriate open source research to be undertaken in establishments and/or regional intelligence hubs as set out below although governors and DDCs will need to take into account the costs and risks of doing this.

Desired Outcomes

1.8 The use of open source research will form an important part of the intelligence and evidence gathering capability in order to prevent or detect crime, prevent disorder, or for the purposes of safety and control. These techniques will be used positively so that relevant information is obtained at the right time. *Furthermore, Managers must have a strategy to share relevant information with Police or other Agencies when appropriate to do so*. Evidence from open source research will be captured, stored, and retained in a manner that can withstand scrutiny in court proceedings.

1.9 *Any open source research will be conducted on appropriate IT and with safeguards in place. Full audit trails must be maintained.* (See Annex D of the official sensitive version of this PSI).

1.10 This PSI also reminds staff of their responsibilities when using social media in a personal capacity, including the need to protect themselves, their family, and colleagues as a result of posts made on Social Network Sites (SNS) or other online comments.

Application

1.11 This PSI is applicable to all establishments, including contracted out prisons. The PSI also applies to staff based in regional offices and NOMS HQ.

Mandatory Actions

1.12 *The Governor or equivalent senior manager in a Regional Intelligence Unit or in HQ must ensure that local policy and processes have the following in place:*

1.13 *All investigations will be in accordance with the law, justified and appropriately authorised.*

1.14 *There must be a full record of all open source research conducted – this is for all levels (see 2.15 – 2.18 below) and the Central Authorities Bureau (CAB) must issue a Unique Reference Number (URN) for all open source research.*

1.15 *Any prison or region undertaking open source research must have a plan approved by the Governor to check that audit trails and computer logs confirm that there has been no unauthorised open source research.*

1.16 *Before there is any research at level 3, 4, and 5, an application must be authorised by the Functional Manager responsible for security/intelligence (at least band 7) or the relevant RIPA Authorising Officer.*

1.17 *All applications at level 3, 4, and 5 must be written and contain the intelligence case with IR references where necessary.*

1.18 *Open Source research at these levels must be conducted by staff in HQ (or regional intelligence unit).*

Resource Impact

1.19 *It is evidently more cost effective if establishments continue to use the central service provided by the Central Authorities Bureau (CAB). However, the PSI is written to allow establishment level or regional level open source capability. This is deliberate during a period when the longer term Agency Intelligence Model is being developed. The critical point is that if open source research is carried out locally or regionally, it must be carried out properly, with appropriate equipment and consistent with the law. If establishments or regions want to purchase equipment for these purposes, they must make a request to NOMS CICT to obtain equipment with the right software and support wrapper*. Initially, they need to email NOMS-CICT-Demand@noms.gsi.gov.ukwith an outline of their request. NOMS CICT will also involve NOMS IA to confirm the necessary compliance structure is in place.

1.20 If establishments continue to use the service offered by NIU, establishment costs will be negligible.

1.21 Due to the costs involved it is likely that central service will be the most cost efficient and most secure method of carrying out this work.

(Signed)

Digby Griffith
Director of National Operational Services, NOMS

2. Operational Instructions

Text within shaded boxes indicates requirements from the "*Provision of a Secure Operating Environment*" bundle of specifications. All instructions below are mandatory.

Local Policy Document

2.1 *Every prison establishment must have a document which is available to staff, prisoners, and visitors stating that all lawful methods will be used for the gathering of intelligence and evidence within the prison.* The use of any intelligence gathering will be undertaken where it is necessary and proportionate to do so.

2.2 *This can be made into a statement and displayed alongside the already mandatory Fair Processing Notice. Governors must also need to issue both a notice to staff and a notice to prisoners.*

2.3 *Governors may wish to draw staff attention again to the Notice to Staff at Annex A of this document. If staff use Social Networking Sites (SNS), they must understand the legalities of what they can post, their responsibilities, and that privacy is not absolute, even when applying security settings to their profile*.

2.4 It is important that staff understand the limits on their investigative capability locally and where there is a need to apply to CAB for more detailed or covert operations.

2.5 *RIPA powers for covert surveillance and CHIS must only be used where the Authorising Officer believes it is necessary for a statutory ground listed in Section 28 (3) or 29 (3) of RIPA and proportionate to what is sought to be achieved.* The statutory grounds are:

- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of public safety.

2.6 *The application processes set out in the covert surveillance and CHIS PSIs must be followed*.

2.7 *Covert surveillance may be undertaken for the purpose of a disciplinary investigation but RIPA powers must not be used for this. (See paragraphs 3.13 – 3.14 and Annex B of the restricted version of PSI 22/2012).*

Intelligence informs actions in the prevention and detection of risks to prison security and the wider community.

2.8 It is important to recognise that open source research is focussed on gathering personal information to fill an intelligence requirement. This process does not need to be followed where Internet research is general or theme based, or is not in any way linked to an intelligence requirement or investigation. In certain cases, as mentioned above, RIPA authorisation will be required.

Security Concerns

2.9 *There must be an audit trail of all open source research.*

2.10 IT Security for this device is outside the scope of the Athena IT Manager and should rest with the Functional Head of Security. *As part of the Security Operating Procedures (SyOps) document, it should be stated any unauthorised access, compromise or other security incident relating to the hardware or software must be reported to the Information Assurance Team as a security incident on 0300 047 6590 as per PSI 24/2014, and also to the CAB.*

Application Process

2.11 Applications can be made from a range of staff such as local or regional corruption prevention managers, investigating officers, security/intelligence staff, or governors. *The key is that the applicant must be the person with sufficient knowledge about the matter under investigation and what the open source application seeks to achieve.*

2.12 *At all times, Applicants must apply appropriate operational controls to ensure that the application is not openly discussed ("the need to know" principle) in order to prevent compromise.*

2.13 *It is essential that at all times, Applicants and Authorising Officers take into account collateral intrusion and do not use open source research as an opportunity to look up information that forms no part of the investigation. Measures must be taken to minimise interference with the private and family life of those not subject of the investigation and decisions documented. Collateral intrusion that occurs must be documented and a plan set out for dealing with it.*

2.14 There are different levels of application, which from level 2 onwards become more intrusive and more likely to require authorisation under the Regulation of Investigatory Powers Act (RIPA).

Level 1: Immediate response

2.15 This is a case which is time critical and is research that is being conducted immediately as a response to intelligence received or an incident and it is believed that personal information held on the Internet will assist. This may be undertaken at an establishment.

Level 2: Information is openly available

2.16 This is information that is available on the Internet and does not require the researcher to have a SNS profile, account, or password to access it. This may be undertaken at an establishment.

Level 3: Information is held in Social Network sites

2.17 Activity from level 3 onwards will be undertaken by HQ or Regional Intelligence Unit.

Level 4 and Level 5 – Covert

2.18 Powers under the Regulation of Investigatory Powers Act (RIPA) apply.

Action taken on Social Network Sites

2.19 There will be occasions that open source research is being undertaken to prove or refute allegations that a prisoner has an active Facebook or other SNS account which has been updated since imprisonment either by the prisoner or a third party.

2.20 *Policy is set out in PSI 49/2011. Paragraph 12.11 of PSI 49/2011 confirms that prisoners must not be allowed to access any social networking site whilst in custody. Third parties* *also cannot update profiles on their behalf. Also, the restrictions on correspondence equally apply to prisoners on temporary release. Where open research is undertaken which confirms that a serving prisoner's SNS profile has been updated since imprisonment, it is for staff in the CAB to make contact with the SNS provider for appropriate action to be taken. Prisons must not make contact with the SNS providers directly but must make an application to the CAB.*

2.21 *In all instances, an Intelligence Report (IR) must be entered into the Mercury Intelligence System (MIS) and other appropriate operational decisions or procedures undertaken.*

Retention Periods

2.22 *All applications, authorisations, and material gathered must be retained for six years from the date of authorisation*. This is in line with the standard approach to retaining intelligence. Information must be managed in line with the DPA, data protection principles, and PSI 24/2014. If the material is shared with the Police for the purposes of a criminal investigation, the material will be managed in accordance with the Criminal Procedure and Investigations Act (CPIA). For more information, see paragraph 3.14 of the restricted version of this PSI.

Hardware

2.23 *As per PSI 25/2014 IT Security and PSI 24/2014 Information Assurance the following must be adhered to. In particular:*

- *Maintain up to date Anti-Virus;*
- *Maintain up to date Anti-Malware;*
- *Maintain all manufacturer issued security updates and patches for all installed software;*
- *Have a nominated administrator and deputy who have this role included on their SPDR. They are responsible for:*

  i. Maintaining a log of users.
  ii. Setting up users with unique logon ID
  iii. Removing users who no longer require access;
- *Any evidence is captured onto an approved encrypted memory stick. – If CD/DVD used instead this will require extra encryption software to be purchased so the CD/DVD can be encrypted. Advice can be given on the level at time of buying through NOMS CICT.*
- *The memory stick must be recorded and uniquely marked and is signed in and out on each use, and data recorded onto log on whose data is on there. This will stop it being overwritten by somebody else. It may be necessary to maintain several memory sticks so each one is solely for a single investigation and to maintain the chain of custody of the evidence. The memory stick must be held in a safe that has controlled access.*

Retaining Evidence

2.24 *Evidence should be retained in PDF and captured on an approved encrypted memory stick.*

2.25 *Where the evidence is a video or other recording, the evidence must be downloaded on to encrypted CD/DVD.*

Annex A

NOTICE TO STAFF

- **Always think before you post.**

Social media is instantly available through mobile devices, making it easy to comment before you have given yourself time to reflect. This can have unintended consequences. Take time to think before you post.

- **Understand the line between what is appropriate and what is not**

Ask yourself whether you would feel comfortable if your manager, colleague, family member or a journalist saw or quoted your post? If the answer is no, don't post it.

- **Know NOMS' rules**

All NOMS staff are expected to familiarise themselves and comply with NOMS' policies, including the following:

The NOMS Conduct and Discipline Policy clarifies the required standard of behaviour, and states that it is not acceptable to bring the Service into disrepute or create an adverse effect on public confidence in the Service. This applies at all times, not simply during working hours or when you are using work equipment.

The NOMS Outside Activities Policy makes it clear that permission is required before publishing (electronically or in hard copy) anything that refers to NOMS official business. This applies even where staff have retired or left the Service for any other reason.

- **Understand the legalities**

You are responsible for everything you post online. The key things to remember are:

  - Don't disclose sensitive or confidential information about other people, your work or your workplace as this could breach the Data protection Act (DPA) or other legislation.
  - Don't make derogatory remarks about prisoners, other individuals, groups or organisations
  - Don't bully harass or discriminate
  - Don't break copyright laws

- **Be aware that your privacy is not guaranteed online**

Your privacy settings do not guarantee that anything you post online will remain private. A Facebook "friend" may pass your comments on.

- **Be careful who you interact with**

Before joining a "group" or affiliating yourself with other organisations and campaigns, check that its views are appropriate for an employee of NOMS and are not incompatible with the values of our organisation.

- **Do not contact the media**

Only authorised staff, normally governing governors and the Ministry of Justice Press Office, are allowed to deal direct with the media. Unless you have specific permission you are not allowed to use online websites or any other means to contact journalists/ the media about any aspects of your employment. All press queries should be referred to the Ministry of Justice Press Office. The NOMS Outside Activities Policy also has further information.

- **Follow the Civil Service Code**

Civil servants are bound by the Civil Service Code. The Code sets out the core values of integrity, honesty, objectivity and impartiality – and the standards of behaviour that are expected of us whether we are online or offline, in work or personal time. It is a good idea to remind yourself of the Code's contents.

- **Do not act online in a way that you wouldn't in day to day life**

For example by being offensive, displaying offensive images, inciting inappropriate behaviour in others, spreading rumours, re-posting offensive information that has been posted by others, or providing official information you are not authorised to disclose. This list of examples is not intended to be an exhaustive list rather to reflect the types of actions it might be easier to take through social media than it would be through other communication channels.

- **Do not become an investigator**

If you come across a member of staff using social media inappropriately do not engage with them, seek to discover more details about them, or attempt to encourage further inappropriate behaviour. Simply report what you have seen (see paragraph 3 below). The same applies should you discover any activity on social media that you believe is connected to a prisoner.

- **Remember**

Staff who do not comply with NOMS' policies or the Civil Service Code face the possibility of investigation and, potentially, disciplinary action.

If your actions are considered to be a criminal offence this could also lead to prosecution.

Anybody who has a concern about inappropriate postings made by staff on social networking sites should report the matter to their line manager, Local Corruption Prevention Manager, or Corruption Prevention Unit via the Wrongdoing Hotline: 01527 544 777.

Annex B

Cabinet Office Guidance

As civil servants, we are all bound by the Civil Service Code. The Code sets out the core values - integrity, honesty, objectivity and impartiality - and the standards of behaviour expected of us.

The simple rule to remember is that the principles covering the use of social and other digital media by civil servants in both a work and personal capacity are the same as those that apply for any other activity. Social media is a public forum and the same considerations would apply as, say, to speaking in public or writing for a publication either officially or out of work. In social media the boundaries between professional and personal are often more blurred - so it's important to be particularly careful.

As civil servants we are (of course) free to use social and other digital media in our own time. But we always need to be mindful of our duties not to disclose official information without authority, and not to take part in any political or other public activity which compromises, or might be seen to compromise, our impartial service to the government of the day or any future government.

We must take care about commenting on government policies and practices and should not do so without the proper authorisation. We should avoid commenting altogether on politically controversial issues and avoid making any kind of personal attack or tasteless or offensive remarks to individuals or groups.

As more and more civil servants are able to access the internet at work both on personal and official devices, it is important that the highest levels of propriety apply at all times. The Civil Service Code applies equally to using personal devices e.g. smart phones, tablets or official devices whether at work or home. We must always act in a way that is to retain the confidence of all the people we deal with.

Further details are available in departmental staff handbooks and Section 4 of the Civil Service Management Code as well as on the Civil Service Learning pages (registration required). Some departments have their own social media policies - civil servants should make sure they are aware of their departments' policy and comply with any departmental restrictions. It's important that we are all aware that posting any content that is considered inappropriate – whether in an official or personal capacity - may result in disciplinary action which could lead to dismissal.