Ministry of Justice

HM Prison & Probation Service

Policy name: Investigatory Powers Policy Framework

Reference: N/A

Issue Date: 1st June 2021 **Implementation Date**: 1st June 2021

Replaces the following documents (e.g. PSIs, PSOs, Custodial Service Specs) which are hereby cancelled:
PSI 22-2012 Covert Surveillance;
PSI 23-2012 CHIS;
PSI 04-2014 Acquisition of Communications Data;

Introduces amendments to the following documents (e.g. PSIs, PSOs, Custodial Service Specs):

Service Specifications altered as noted in Appendix 5.2.

Action required by:

☒	HMPPS HQ	☒	Governors
☒	Public Sector Prisons	☒	Heads of Group
☒	Contracted Prisons	☐	Contract Managers in Probation Trusts
☒	National Probation Service	☐	Community Rehabilitation Companies (CRCs)
☒	HMPPS Rehabilitation Contract Services Team	☐	HMPPS-run Immigration Removal Centres (IRCs)
☐	Other providers of Probation and Community Services	☒	Under 18 Young Offenders Institution

Mandatory Actions: All groups referenced above must adhere to the Requirements section of this Policy Framework, which contains all mandatory actions.

For Information:

Governors must ensure that any new local policies that they develop because of this Policy Framework are compliant with relevant legislation, including the Public-Sector Equality Duty (Equality Act, 2010).

How will this Policy Framework be audited or monitored: Review by National Intelligence Unit, Regular reporting to Senior Responsible Owners for RIPA and IPA

Resource Impact: None

Contact: Centralauthoritiesbureau@justice.gov.uk

Deputy/Group Director sign-off: Claudia Sturt, Director, Security, Order and Counter terrorism, HMPPS.

Approved by OPS for publication: Ian Barrow and Sarah Coccia, Joint Chairs, Operational Policy Sub-board.

CONTENTS

1. Purpose

1.1. Purpose of Policy Framework

The policy will ensure consistent application of powers available to HMPPS under the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA).

1.2. Guidance and additional instructions for Operational staff

Detailed guidance for operational staff working in any areas affected by this Policy Framework will be provided via a restricted Operations Manual which has been restricted in order to protect HMPPS tactics from exposure. This will be provided to relevant staff by the National Intelligence Unit.

1.3. Legal basis for Investigatory Powers within HMPPS

HMPPS has powers under the Acts listed above and the associated Codes of Practice, to enable activity to be conducted aimed at the prevention and detection of crime, preserving order and discipline in establishments and management of risk and prevention of harm as well as any duty or responsibility arising from common law or other legislation. Specific to this Policy Framework are the powers to:

- **Acquire Communications Data** – to identify illicit communications devices being used illegally inside prisons or in contravention of licence conditions, and to help identify criminal activities in prisons through the illicit use of mobile phones.
- **Conduct Surveillance –** to combat criminality within prisons, maintain order and discipline, or to support the gathering of information and intelligence for the purposes of pursuing a prosecution/adjudication.
- **Deploy Covert Human Intelligence Sources (CHIS) –** To gather intelligence and information to assist in the detection and prevention of crime, maintain good order and discipline, and reduce the risk of harm to vulnerable people.

The power to intercept communications under s49 of the Investigatory Powers Act 2016 is covered by PSI 04/2016 – Interception of Communications and Security Measures in Prisons.

1.4. Assurance and Governance for Investigatory Powers within HMPPS

Each of the powers available to HMPPS is overseen by a Senior Responsible Owner (SRO), who are supported in this role by a function which provides the central retrievable record.

- The Senior Responsible Owner for powers under RIPA 2000 is the Director of Security, Order and Counter Terrorism (SOCT) or other nominated Senior Civil Servant. The central record function is provided by the National Intelligence Unit.
- The Senior Responsible Owner for Communications Data and Internet and Intelligence Investigations is the Deputy Director (National Security Group) of SOCT, or other nominated Senior Civil Servant or delegated official. The central record function is provided by the National Intelligence Unit.

2. Outcomes

2.1. Policy Aims

2.1.1. All staff in HMPPS and the Contracted Estate understand what constitutes investigative activity, and their legal obligations under the relevant legislation

2.1.2. HMPPS deploys investigative powers when necessary and justified, proportionate to the outcomes being sought, including the consideration of less intrusive tactics and capabilities.

2.1.3. Applications for use of Investigatory powers are submitted in the correct manner, authorised following proper scrutiny, managed for the lifetime of the authorisation robustly, and data managed appropriately until deletion.

3. Requirements

3.1. Applications and use of Investigatory Powers

3.1.1. The use of Investigatory Powers may engage the rights contained in Article 8 of the European Convention on Human Rights. All applications for the use of such powers must consider how this article is engaged, and ensure that the correct processes are followed to ensure that investigatory activity is carried out within the proper framework.

3.1.2. All HMPPS staff applying to make use of Investigatory Powers under this Policy Framework must use the approved forms and processes set out in the restricted Investigatory Powers Operations Manual.

3.1.3. Any activity which is not compliant with this Policy Framework, or the Operations Manual must be reported to the Central Authorities Bureau (CAB). This activity will be considered by the Head of CAB or delegated officer within 5 working days to decide if a relevant error as defined in the relevant Code of Practice has been committed, and if required submit a report of the incident to the Investigatory Powers Commissioners Office (IPCO). Examples of breaches which must be reported are included in the relevant sections below

3.2. Acquisition of Communications Data

3.2.1. Governors and senior managers must ensure that HMPPS seek to acquire communications data (CD), only where it is necessary and proportionate to do so for the following statutory purposes under the Investigatory Powers Act 2016

- The applicable crime purpose, (S60A(7)(b) and / or S61A(7)(a)
- In the interest of public safety, (S60A(7)(d) and / or S61A(7)(b)

3.2.2. All communications data held by telecommunications and postal operators falls into three categories:

- Entity data – Describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects. (e.g. subscriber check of a phone number)
- Events data – Describes or identifies events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time. (e.g. itemised call records)
- Internet Connection Records – this describes a record of an event about the service a user has connected to on the internet. (E.g. accessing an internet service or application).

Events data is considered the most intrusive data set, and as such the applicant must ensure the serious crime threshold (as set out in the Operations Manual) is met.

3.2.3. Applications under section 60A must also be necessary for:

- a specific investigation or operation for one of the purposes listed at paragraph 3.2.1; or

- for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data,

The conduct authorised must be proportionate to what is sought to be achieved.

3.2.4. For applications under section 61A:

- it must be necessary to obtain the data for a specific investigation or a specific operation for one of the purposes listed at paragraph 3.2.1;
- there must be an urgent need to obtain the data; and
- the conduct authorised must be proportionate to what is sought to be achieved.

3.2.5. Applications for CD must be submitted following the process set out in the Investigatory Powers Operations Manual, to the HMPPS Single CD Point of Contact (SPoC) who will submit applications to the Office of Communications Data Authorities (OCDA**). It is advised that applicants; especially if they do not have experience in this requesting communications data, contact DMIU in the first instance prior to submitting an application.** They will provide a Unique Reference Number (URN) and if needed the most up to date version of the form.

3.2.6. The CD SPoC acts as a 'guardian and gatekeeper' to ensure that public authorities act in an informed and lawful manner. They must have completed the required CD accredited training in order to submit applications to OCDA for consideration (s60A). SPoCs formally request data from Telecommunications Operators and Postal Operators on behalf of HMPPS.

3.2.7. HMPPS also has a Designated Senior Officer (DSO), who can grant an authorisation to acquire certain types of communications data (entity data) for specified purposes in cases where there is an **urgent** need to acquire the data (Section 61A). The identified DSO for HMPPS is the Head of DMIU, or in their absence, individuals more senior within the National Security Group line management chain in the SOCT Directorate.

3.3. **Surveillance**

Subject to the constraints at 4.4 Governors and/or Heads of Regional Units are responsible for ensuring that:

3.3.1. All applications for surveillance are submitted on the grounds permitted under Section 28(3) of RIPA 2000, which for HMPPS are:

(b) for the purpose of preventing or detecting crime, or of preventing disorder
(d) in the interests of public safety

3.3.2. All applications for surveillance, regardless of the legal basis for the application, must be submitted using the forms and processes outlined in the Investigatory Powers Operating Manual, and authorised by the appropriate officer as identified in section 5.1 of this policy.
Surveillance is Directed Surveillance where the following are all true:

- It is covert;
- it is conducted for the purposes of a specific investigation;
- it is likely to result in the obtaining of private information about a person; and
- it is not conducted as part of immediate response to an incident.

Intrusive surveillance is covert surveillance that is:

- carried out in relation to anything taking place on residential premises (which includes prison cells); or
- in any private vehicle, and
- involves the presence of an individual on the premises or in the vehicle, or is carried out by a means of a surveillance device
- carried out in relation to a legal consultation

3.3.3. Applications for directed and intrusive surveillance follows the guidance provided by the National Intelligence Unit, which will ensure that applications contain the information required by section 28 RIPA and as described in section 5.6 of the Covert Surveillance and Property Interference Code of Practice 2018 to enable the Authorising Officer to decide if:

- the proposed surveillance is necessary on one of the grounds in section 3.4.1,
- and proportionate to what is sought to be achieved.

3.3.4. All covert surveillance (directed or intrusive) is carried out in accordance with RIPA 2000, and only once authorised by an officer permitted to authorise under section 3.6 of this framework.

3.3.5. Overt CCTV is not used for the purposes of covert surveillance conducted for the purposes of a specific investigation or operation without an authority for Directed or Intrusive Surveillance being granted.

3.3.6. Use of overt CCTV cameras for constant observation of prisoners under Prison Rule 50A/YOI Rule 54 is authorised, logged, and monitored, to ensure that collateral intrusion is minimised, or be considered as to whether an application for directed surveillance is required. Use of the powers under Prison Rule 50A must only be for the maximum duration specified in the guidance issued by the CAB.

3.3.7. Errors, breaches and compromises of Surveillance operations are reported immediately to CAB. Examples that must be reported include, but are not limited to the following. If there is any doubt the CAB must be contacted to discuss:

- Deployment of covert surveillance without authorisation
- Any identification of staff by prisoners or non-included staff as being involved in a surveillance operation
- Exposure, accidental or deliberate, of covert surveillance equipment
- Disclosure to the target(s) of a surveillance operation that they are under surveillance
- Loss of any paperwork or electronic files relating to surveillance operations, including the Operations Manual
- Disclosure of intelligence or material obtained through covert surveillance without the permission of the Authorising Officer

3.4. <u>Covert Human Intelligence Sources (CHIS)</u>

Subject to the constraints in 4.5 Governors and/or Heads of Regional Units are responsible for ensuring that:

3.4.1. Inducing, asking or assisting a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS within establishments as well as conduct of the CHIS are authorised in accordance with section 29 RIPA and otherwise are compliant with RIPA 2000 and the relevant codes of practice. 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 falling within paragraph 3.5.1.2 or 3.5.1.3;
- 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.

3.4.2. All applications for CHIS are submitted on the grounds permitted for HMPPS' use of CHIS under Section 29(3) of RIPA 2000, which are:

(b) for the purpose of preventing or detecting crime, or of preventing disorder
(d) in the interests of public safety

3.4.3. Applications for recruitment and authorisation of CHIS are submitted using the correct forms and processes laid out in the Investigatory Powers Operations Manual, and authorised by the appropriate officer as identified in section 5.1.

3.4.4. Applications for use of CHIS follows the guidance provided by the National Intelligence Unit, which will ensure that applications contain the information required in section 29 RIPA and section 5.11 of the Covert Human Intelligence Source Code of Practice 2018 to enable the Authorising Officer to decide if the proposed use of CHIS is:

- Necessary on one of the grounds in section 3.4.2;
- The proposed conduct and/or use is proportionate to what is sought to be achieved; and
- That arrangements are in place which satisfy the requirements set out in section 29(4A) and 29(5) of RIPA and any other requirements imposed by orders made by the Secretary of State (e.g. where a child or vulnerable person is used as a CHIS)

3.4.5. No HMPPS CHIS is authorised without knowledge of the Central Authorities Bureau, and submission of the appropriate forms.

3.4.6. All required forms for reviews, renewals and cancellations are completed in a timely fashion, and submitted to HMPPS CAB no later than 3 working days after the date of the event.

3.4.7. HMPPS staff who are delivering statutory roles must have attended the appropriate training, and that such staff have attended the required refresher training within specified periods. This must include ensuring that there are sufficient individual officers able to act as the persons identified in Section 29(5)(a) and (b) RIPA 2000.

3.4.8. Appropriate information security measures are in place to store and protect CHIS documentation.

3.4.9. Any claim made by an individual to currently be or previously have been authorised as a CHIS is reported immediately to CAB.

3.4.10. Any request for information regarding the alleged or potential use of an individual, past or present, as a CHIS is referred immediately to the CAB, who will respond with a “neither confirm nor deny” statement, subject to the constraints in 4.5.4.

3.4.11. Errors, breaches and compromises of CHIS operations are reported immediately to CAB. Examples that must be reported include, but are not limited to the following. If there is any doubt the CAB must be contacted to discuss:

- Any identification of staff by prisoners or non-included staff as being involved in a CHIS operation (e.g. being a Handler, Controller etc.)
- Identification of a source, either accidental or deliberate by prisoners, public or non-included staff
- Disclosure to the target(s) of a CHIS operation that they are under suspicion, even if the intelligence collection tactic is unknown
- Loss of any paperwork or electronic files relating to CHIS operations, including the Operations Manual
- Disclosure of intelligence or material obtained through CHIS without the permission of the Authorising Officer

3.5. **Authorising Officers**

3.5.1. Authorising Officers (AO) will be appointed for all activity covered by this policy framework in accordance with the relevant legislation.

3.5.2. HMPPS CAB will retain a list of approved AOs for all Investigatory Powers activity. The list will detail which specific activities that individual AO is able to authorise. Any person not on that list, is unable to authorise activity covered by this policy framework, regardless of previous training or experience.

3.5.3. Authorising Officers for all standard level authorities must complete the required training, and complete a minimum number of authorities per year as directed by the Director of Security, Order and Counter-Terrorism (or successor posts), who may delegate this direction to the HMPPS Head of Intelligence.

3.5.4. Authorising Officers will ensure that authorisations are only granted for the duration permitted in legislation. These are summarised in section 5.1

3.5.5. Authorising Officers for RIPA authorities must, in liaison with the applicant, review each authority granted on a regular basis, or following a change in circumstances, to ensure that it remains necessary and proportionate. The initial review for CHIS and Surveillance must be completed no later than one month after authorisation, but can be sooner.

3.5.6. If at the time or review the authorisation is no longer necessary and proportionate the Authority must be cancelled by the Authorising Officer.

3.5.7. All reviews, renewals and cancellations must be considered if possible by the Authorising Officer who granted the original authority. Where this is not possible the CAB will provide guidance.

3.6. Staff

3.6.1. Governors and Heads of Units must give careful consideration to the identity and character of staff involved in the deployment of any powers under this framework.

3.6.2. Staff for whom RIPA activity is the total or majority of their roles must hold National Security Vetting Level – Security Check (SC) as a minimum.

3.6.3. Governors and Heads of Unit should consider requiring all staff inducted into CHIS and Surveillance operations to be subject to a minimum of SC clearance.

3.6.4. If a member of staff involved in delivery of any activity under this Policy framework is identified by any individual (including staff or prisoners) who is not included in the operation, or does not need to know about the staff members' role, then that compromise must be reported immediately to CAB. If a RIPA operation is ongoing, a risk assessment must be undertaken and the Authorising Officer informed. CAB will maintain a register of compromises.

3.7. Investigatory Powers Commissioners Office (IPCO)

3.7.1. HMPPS use of Investigatory Powers is subject to inspection by IPCO. When satisfied that the requestor is a bona fide employee of IPCO, any request for access to information in connection with these powers must be complied with.

3.8. Law Enforcement Agency (LEA) Investigatory Powers activity within Prisons

3.8.1. Under RIPA 2000 police have the ability and powers to undertake surveillance and CHIS deployment within prisons. All such activity must be notified to CAB to enable effective management of risk and efficient deployment of resources.

4. Constraints

4.1. Retention of Information

4.1.1. All records pertaining to the use of Investigatory Powers must be managed and destroyed in line with PSI 04/2018 - Records, Information Management and Retention Policy

4.1.2. The Central Record Function identified in section 1.4 will be responsible for destruction of the information held on the central record at the appropriate point, and will issue reminders to local and regional staff responsible for holding records to destroy records at the same point.

4.2. Obtaining of Legally Privileged or confidential information

4.2.1. Any operation which is likely to, or deliberately seeks to obtain legally privileged or confidential information is subject to enhanced authorisation regimes, set out in section 5.1. Where an operation obtains such information inadvertently, the Authorising Officer and CAB must be informed immediately, to enable instructions to be issued for the further handling or destruction of the material obtained.

4.2.2. Such material obtained inadvertently can only be retained or shared where the Authorising Officer believes there is evidence of intention to further criminal activity. In all such instances a legal advisor will be contacted immediately by the NIU for advice.

4.2.3. All such material retained will be reported to IPCO in line with the relevant Codes of Practice.

4.3. Acquisition of Communications Data

In addition to the requirements in section 3.2, all staff must note:

4.3.1. Applications for Communications Data under the Investigatory Powers Act 2016 cannot be submitted by any person in HMPPS apart from accredited DMIU CD SPoCs. Attempts to do so will result in applications being returned by OCDA. Telecommunications and Postal Service providers will not supply any CD to a non-accredited SPoC and function. Any attempt to obtain CD by any other person will be regarded as constituting unlawful attempts to obtain data.

4.4. Surveillance

Further to the requirements in section 3.3:

4.4.1. The following are regarded as intrusive for the purpose of this Policy Framework, and therefore require higher levels of authorisation, detailed in Appendix 5.1:

- Surveillance within a cell or private vehicle
- Surveillance of legal visits

4.4.2. HMPPS may only use powers under RIPA to conduct covert surveillance where necessary and proportionate:

- for the purpose of preventing or detecting crime or of preventing disorder; or
- in the interests of public safety.

Therefore, covert surveillance must not be used to investigate a matter that will be subject to disciplinary matters only (e.g. secondary employment).

4.4.3. Staff must be aware that there are activities which can drift into Directed Surveillance activity. These include:

- Online Research – HMPPS staff not trained in Internet Investigation must not undertake surveillance, for example, by monitoring of social media profiles. Where it is identified that online information may be of use, advice must be sought from the DMIU immediately. DMIU provide a 24/7 on call service to support any serious incidents involving prisoners posting online content.
- Constant observation of prisoners under Prison Rule 50A/YOI Rule 54– Sustained use of CCTV cameras to monitor an individual may drift into surveillance, advice should be sought from CAB
- Targeted use of overt CCTV cameras – Overt cameras being used for covert purposes should be always be considered for a Directed Surveillance application

4.5. **CHIS**

Further to the requirements in section 3.4:

4.5.1. No officer is permitted to disclose the identity of a CHIS to any person, without the express permission of the Authorising Officer, or the Senior Responsible Owner. Any compromise of a CHIS identity must be reported immediately to the Authorising Officer and the CAB.

4.5.2. The following use of CHIS requires a higher level of Authorising Officer, detailed in Appendix 5.1:

4.2.3.1. Where the use and conduct is to obtain or disclose confidential communications between a person and an MP, Journalist, Doctor or religious advisor.

4.2.3.2. Where the use and conduct is to obtain or disclose information subject to legal privilege.

4.2.3.3. Where the CHIS is defined as vulnerable as per section 4.1 of the Codes of Practice

4.2.3.4. Where the CHIS is under the age of 18. HMPPS will not authorise use of CHIS under the age of 16.

4.5.3. A CHIS wearing or carrying a surveillance device does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the CHIS, and the use of the device is explicitly included in the scope of the CHIS authorisation. However, if a surveillance device is to be used other than in the presence of the CHIS, an intrusive or directed surveillance authorisation should be obtained where appropriate.

4.5.4. A text confirming or denying any assistance provided by an individual to HMPPS can only be issued by the CAB. No other officer or person can provide such a text unless expressly authorised to do so by the Head of CAB. The potential recipients of such texts include, but are not limited to:

- Parole Board
- Courts
- Any other Court like body (including but not limited to Employment Tribunals)
- Any other internal or external forum (including but not limited to Multi Agency Public Protection Arrangements, IPP and Lifer Progression Panels).

5. Appendices

5.1. Authorising Officers Table

Activity	HMPPS application
Deployment of CHIS in prison (Standard and Urgent)	A trained and approved (as per 3.5.2) officer of Band 8 or above, employed by HMPPS, responsible for the prison where the CHIS is being deployed, or an officer of a higher grade than that manager operating in a regional capacity.
Juvenile (under 18) CHIS	Deputy Director or above
Vulnerable CHIS	Deputy Director or above
CHIS obtaining/disclosing confidential information	HMPPS CEO
CHIS obtaining/disclosing legally privileged material	HMPPS CEO
CHIS authorised to participate in criminal activity as part of tasking	Band 10 or above in National Intelligence Unit
Directed Surveillance in prison (Standard and Urgent)	A trained and approved (as per 3.5.2) officer of Band 8 or above, employed by HMPPS, responsible for the prison where the surveillance is to be carried out, or an officer of a higher grade than that manager if operating in a regional capacity.
Directed Surveillance likely to obtain confidential or legally privileged material	HMPPS CEO
Intrusive Surveillance in Prisons (e.g. in cell, legally privileged activity)	Secretary of State
Acquisition of Communications Data	Office for Communications Data Authorisations (OCDA) AO via HMPPS Single Point of Contact (SPoC)
Urgent Acquisition of Communications Data	Designated Senior Officer (DSO) or a national senior manager in National Security Group in their absence
Standard Application for Internet Intelligence Investigation	Band 7; or equivalent in a contracted prison
Deployment of CHIS or Directed Surveillance in a Contracted Prison	MOJ Controller responsible for the prison, or an officer of a higher grade operating in a regional capacity If urgent – Deputy Controller.

5.2. **Duration of Authorisations**

Power	Activity	Duration	Example Expiry if start date 09:00 10th March
CHIS	Written Authorisation	12 months, minus 1 day	23:59 9th March
	Juvenile CHIS	4 months	23:59 9th July
	To obtain legally privileged material	3 months	23:59 9th June
	Urgent Oral authorisation	72 hours	08:59 13th March
Surveillance	Written Authorisation	3 months	23:59 9th June
	Urgent Oral authorisation	72 hours	08:59 13th March

5.3 Service Specifications impacted by this Policy

The table identifies specifications which are impacted by this Policy Framework (PF) in the following ways:

- **Mandatory Instruction** – The PF includes instructions which, if not followed, would prevent delivery of the specification
- **Supports** – The PF provides instruction/details which when implemented will enable the delivery of the specification
- **Replaces –** The PF includes instructions which supersede the specification due to new products/processes or systems

Service Specification	**Section(s)**	**Impact** (relevant sections of policy hyperlinked if applicable)
Security Management	24	Supports (Surveillance)
	25	Supports (CHIS)
	26	Supports (Investigatory Powers Operations Manual)
	33	Supports (Intelligence Collection, Analysis and Dissemination Policy Framework)
Provision of Secure Operating Environment – Communication and Control Room	8	Supports (Surveillance)
	11	Supports (Surveillance)