Corporate Policy | Service Instruction

SI0425

Covert Records Management

SI Identification Number	SI0425
Policy Ownership	Crime Department
Initial Publication	27 October 2025
Review Cycle	Annually
Reviewed	N/A
Last Amended	N/A
Governing Service Policy	Information Management
Cancellation of	N/A
Classification	**OFFICIAL [PUBLIC]**

The purpose of this Service Instruction is to assist in discharging the Chief Constable's responsibilities arising from the authorisation and use of covert and investigatory activity which are likely to result in the PSNI recording, acquiring or maintaining material or data related to members of the public.

Table of Contents

Table of Appendicies

1. Introduction

The Police Service of Northern Ireland (PSNI) is committed to ensure compliance with the statutory Codes of Practice governing the authorisation and use of covert powers, which includes a requirement for effective procedures to manage the records and product of covert activity and authorisations.

PSNI will manage covert records to comply with its legal, statutory and other obligations including, but not limited, to:

- Police Act 1997;
- Regulation of Investigatory Powers Act 2000;
- Investigatory Powers Act 2016;
- Communications data Code of Practice (2018);
- Interception of Communications Code of Practice (2022);
- Equipment Interference Code of Practice (2018);
- Covert Human Intelligence Source Code of Practice (2022);
- Covert Surveillance and Property Interference Code of Practice (2014);
- PSNI Records Retention & Disposal Schedule;
- Interception of Communications Codes of Practice and;
- Other relevant legislation and industry standards.

The cumulative effect of these provisions and Codes are that there are obligations placed on the PSNI to retain, review and where appropriate dispose of material acquired in the course of covert or investigatory activity. Until disposal, the material must be safeguarded for an authorised purpose.

This Service Instruction applies to the following activity:

- To ensure the security of the data and information we own, hold and are entrusted with; and
- To ensure we fully utilise data and information to improve the effectiveness and efficiency of our service and keep people safe.

Our vision is to ensure that the Police Service of Northern Ireland's acquisition, use, retention, disclosure and disposal of data and information enhances our

legitimacy, the trust and confidence of those we serve and makes Northern Ireland safer for everyone.

The new data Data and Information Risk Strategy sets out the strategic vision and three key strategic objectives by which we aim to ensure that a culture exists where data and information is managed, processed and disposed of ethically, securely, and effectively in line with national Policing standards, our legal obligations, and the public's expectations to enhance legitimacy, trust and confidence in Policing.

Our strategy is built around three key Strategic objectives:

- To ensure the Police Service of Northern Ireland's data and information acquisition, use, retention, disclosure and disposal is lawful, ethical and accountable.

This Service Instruction applies to the following activity:

- Acquisition of Communications Data;
- Surveillance and Property Interference;
- Covert Human Intelligence Sources;
- Targeted Equipment Interference; and
- Targeted Interception.

This Service Instruction supports wider organisational Records Management as set out in SI0419 Records Management.

2. What is a Covert Record?

A covert record refers to intelligence or product, (either in digital or hard copy format) gathered through surveillance and or covert techniques which have been conducted without the knowledge of the subject being monitored and incorporates:

- An authorisation for covert or investigatory powers under RIPA, IPA, or Police Act 1997;
- The product deriving from any authorisation under RIPA, IPA, or Police Act 1997 which includes Communications Data;
- Other records of an administrative and supporting nature relating to the use of covert or investigatory powers under RIPA, IPA, or Police Act 1997;
- Product or authorisations received from other public authorities or law

enforcement bodies whether within the UK or abroad.

Where a record is obtained covertly, and it is later transferred or disseminated through an evidential or opening up disclosure process, for example; transforming raw intelligence into a format that can be used as evidence in legal proceedings; that record is to be treated as an overt item and no longer a covert record under this Service Instruction.

3. Responsibilities

Senior Responsible Officer (SRO):
The SRO for the Police Service of Northern Ireland is the Deputy Chief Constable.[1]

The SRO has the overall responsibility to ensure compliance with this Service Instruction and the relevant statutory Codes set out in Section 1 - Introduction. The SRO will be supported by the Detective Chief Superintendent, Covert authorisations bureau.

The SRO will ensure the 'pathways' for such material are documented and regularly reviewed in line with best practice guidance. The SRO shall ensure accountability at all levels of this process.

Authorising Officers (AO's):
The AOs will authorise the use of most covert powers and provide oversight and support for higher level authorities prior to formal CAB submission to Chief Officers. The AO has an important role in overseeing the management of the covert authorities and in particular considerations in respect of privileged or confidential material acquired during the use of those warrants and authorisations. Designated D/Superintendents will be appropriately trained and skilled to perform the role and function on behalf of the Police Service.

Responsible Officer (RO)
The RO is Detective Chief Superintendent, C5 and will, on behalf of the SRO, undertake the day-to-day interim duties of the SRO to provide assurance that the organisation is compliant with this policy and associated legal frameworks governing covert data.

[1] For Communications Data the SRO is D / Supt Digital Intelligence Hub

Communications Data Single Point of Contact (SPoC)

The SPoC is appropriately trained to facilitate the lawful acquisition of Communications Data and effective co-operation between Public Authorities, Telecommunications Operators, Postal Operators and IPCO Authorisations (where required). To become accredited an individual must complete a bespoke course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier.

The SPoC role promotes efficiency and good practice in ensuring only practical and lawful applications for Communications Data are progressed. Importantly, the role provides objective judgement and advice to applicants and those handling Communication Data.

The SPoC will assist in the overall management of Communications Data ensuring safeguards are complied with in accordance with the Codes of Practice and this Policy.

Senior Investigating Officer (SIO)

The SIO has managerial responsibility for material gathered in relation to criminal investigations conducted within their area of responsibility in strict compliance with the obligations set out in Section 1 - Introduction. Accountability for compliance and adherence to this Service Instruction and the requirements of the relevant Codes of Practice will be held in collaboration between the SIO, Applicant, Investigating Officer, Disclosure Officer and as appropriate, the Authorising Officer.

The SIO is responsible for oversight and monitoring of the discharge of these core responsibilities.

Applicant

Under the supervision of the SIO, the Applicant will manage the retention, review and disposal of material held on bespoke management and workflow systems. These responsibilities may be transferred to other nominated individuals throughout the lifecycle of acquired material.

Responsibilities under the Criminal Procedure and Investigation Act 1996 (CPIA) are not affected by this Policy and therefore remain with the Applicant and the Product Managers.

Applicants should be aware of the specific requirements of those engaged in certain professions e.g., a medical doctor, lawyer, journalist, member of a relevant legislature, or minister of religion and must document

how the application, and any resultant material will be handled.

Covert authorisations bureau (CAB)
CAB is responsible for processing all covert applications in The Police Service of Northern Ireland with the exception of applications for communications data and targeted interception. CAB will also provide advice and guidance for Officers and Staff across the Service.

The role of CAB personnel is to quality assure covert applications, the majority of which are submitted on bespoke management and workflow systems for which the Staff have administration rights.

CAB personnel will play an integral part in ensuring recipients of data are aware of their records management responsibilities.

CAB will also oversee the review of legacy material acquired prior to 2018 with the support of the Responsible Officer.

Operational Security Advisor (OPsY)
The OPsY will provide advice and support in respect of emerging issues and propose new strategies / processes to improve the effectiveness and security of covert operations. The overarching objective will be to ensure that standards are maintained and good practice and learning are identified and shared. The OPsY is supported by a network of Operational Security Liaison Officers (OSLOs) within each Branch and units.

OPsY has a remit to examine any covert operation or process and make recommendations to the AO and or SIO for remedial action. OPsY will also assist with IPCO inspections, and any out of external enquiries relating to covert methodology.

4. Governance

The table below sets out the identified roles with responsibility in relation to this Service Instruction.

ROLE	RESPONSIBILITY
Data Controller	Chief Constable
Senior Responsible Officer	Deputy Chief Constable
Senior Information Risk Owner	Deputy Chief Constable
Responsible Officer	Detective Chief Superintendent C5

Information Asset Owner	Heads of Branch
General Management and Oversight	Detective Superintendent **or** Detective Chief Inspector SPoC within each Branch
Compliance Responsibilities	All personnel accessing covert records

The Covert Data Group, chaired by the Responsible Officer, has responsibility for monitoring compliance and implementing any required changes to PSNI practice as a result of changes in operational practice or legislative change. Key task and finish groups as required will support this group to ensure operational and organisational consistency.

Individual Heads of Branch and or District Commanders using covert or investigatory powers shall be accountable to the Covert Data Group for the management of Covert Data.

The Responsible Officer will be accountable for this function to the Service Data Board, where issues may be escalated to for decision or ratification by the Board or SIRO / SRO in closed session.

All Staff and Officers involved in the use of covert and investigatory powers shall be familiar with their responsibilities under this Service Instruction and the associated Codes of Practice.

5. Key Safeguards

The relevant Codes of Practice for covert authorities contain safeguarding provisions intended to ensure the clear ownership, dissemination, copying, retention and disposal of material obtained is kept to the minimum periods necessary and for a lawful Policing purpose.

Covert Data - Key Safeguards	
Ownership	• The Police Service will understand what covert data product it has obtained, where those records are secured and the justification period for continued retention; • Covert Data pathways will be clearly documented and reviewed annually; • Ownership of all covert data will be clearly identified and maintained throughout the lifecycle of the data; • All records created during the course of day-to-day business are owned by the Police Service and not the individual who created them.
Dissemination	• The number of persons with access to material should be constrained to the minimum necessary to achieve the statutory purpose and aims. Where covert data is held electronically, clear access control policies should restrict access and be regularly reviewed.
Copying	• Material may only be copied to the extent necessary for an authorised purpose, provided for by law, which includes extracts and summaries of material.
Retention	• Material including copies, extracts and summaries must be handled and stored securely to minimise the risk of loss or theft. If material is retained, it should be reviewed at appropriate intervals to confirm the justification for its retention is still valid.
Disposal	• Product or information that has been obtained covertly will be subject to review and deleted once there is no longer a lawful Policing purpose for its continued retention.

6. Ownership of Covert Data

Ownership of covert data will be based on role and function. Where a function or role transfers to another unit or team the ownership of the relevant data will transfer also. In general the Information Asset Owner will own the authorities for the covert or investigatory powers, however the product and records may be held by other departments or units.

7. Retention & Review

All covert data material must be subject to a meaningful review process post-operation and due consideration decisions recorded for the need for further retention and or disposal. When undertaking this review exercise, Authorised Professional Practice highlight that the presumption should be that record(s) should be deleted, unless a reason is found that justifies retention for a Policing purpose. Only the minimum amount of material should be retained to satisfy that purpose.

Where material is retained there must be regular meaningful reviews of material to consider the nature of the material and to ensure information and records are only retained for as long as there is a lawful Policing purpose.

At the conclusion of each covert operation or cancellation of a covert authority, and within one calendar month, the Authorising Officer and / or SIO will be responsible for ensuring the completion of a Covert Data Schedule detailing what covert data exists in relation to that operation or authority. When completing the schedule the AO and SIO will identify what covert data is:

- Authorities;
- Product;
- Records (non-authorities/product);
- Considered irrelevant and or suitable for immediate disposal.

There are different requirements for the various covert and investigative powers. CAB personnel will quality assure the scheduling of covert data in relation to covert authorisations on a regular audit and compliance basis.

Heads of Branch and District Commanders shall ensure that all covert data is appropriately stored and recorded in line with the data pathways.

8. Evidential Product

This Service Instruction applies only to those covert records which are being managed outside of the evidential chain. Ensuring the continuity and integrity of potential evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are important considerations as part of the disclosure process under the Criminal procedure and Investigations Act 1996. Existing mechanisms apply to ensure the appropriate disclosure considerations in respect of opening up or converting raw covert product into an evidential format. CPIA 1996 will subsequently govern the retention, review and disposal of those records and this Service Instruction will cease to have effect in respect of that product. However, it will continue to have effect for the remaining connected records (authorisations, supporting and administrative records) which enabled the lawful provision of the product.

Product obtained as a result of Targeted Interception and Targeted Equipment Interference is subject to additional safeguarding processes beyond CPIA 1996. Unauthorised disclosure of the existence of a warrant, or any product, is a criminal offence under Section 59 Investigatory Powers Act 2016. Similarly these are ordinarily inadmissible in Court proceedings. Enhanced arrangements are in place to manage these records and product on behalf of the organisation.

9. Disposal Process

Following the conclusion of an operation, arrangements must be in place to expeditiously undertake a meaningful review exercise mandated as part of the CAB Scheduling Directive. This review must record a clear rationale by the Reviewing Officer / Staff member as to whether covert data is deemed suitable for further retention in line with this Service Instruction.

Where the decision is made that covert data is suitable for disposal, a notification will be sent to the SIO[2], by the person deciding the material is suitable for disposal, which sets out the intention to delete the covert data. This will allow any representations as to whether there are any further grounds to retain data beyond the identified retention period.

[2] Heads of Branch should ensure there are appropriate arrangements in place for reviews where the SIO is no longer in Service.

Where the SIO is no longer in service the views of the Information Asset Owner will be consulted.

The SIO / Information Asset Owner will have 30 days to make representations on why the covert data should be retained for longer. In cases of disagreement, the Responsible Officer shall determine whether the material will be retained or not.

If no representations are made - any material considered suitable for disposal should be disposed following the expiry of relevant retention periods as set out in this Service Instruction. When information and records are no longer required, or have reached the end of their designated retention period, arrangements must be in place to ensure that appropriate methods are used for their disposal and accurate records of destruction retained.

When considering disposal of CHIS data, the responsibilities of the SIO under this section shall be performed by the relevant AO at the time, in consultation with the SIO(s) as appropriate.

Where disposal is authorised, covert data must be destroyed such that it is impossible to access, including any duplications of data that may exist across electronic systems.

10. Partner Covert Data

The Police Service works in collaboration with a broad range of investigatory and law enforcement partners. Where in the course of joint working the Police Service receive either:

- An authorisation for covert or investigatory powers under RIPA, IPA, or Police Act 1997 provided by a Partner Agency; or

- The product deriving from any authorisation under RIPA, IPA, or Police Act 1997 which includes Communications Data received by a Partner Agency.

The Officer or Staff member within the Police Service of Northern Ireland receiving that shall take such steps as to record, protect and safeguard that data in line with this Service Instruction. In particular they shall ensure:

- All covert authorisations (including communications data authorisations) are notified and shared with the Police Service's Covert authorisations bureau;

- Take steps to safeguard any covert product received from partners in line with the relevant Codes of Practice;
- Any joint material held by the Police Service of Northern Ireland will also be subject to appropriate review, retention and scheduling arrangements; and
- Disposal decisions in respect of any partner owned records will be subject to joint consideration and agreement between the respective leads.

11. Error Reporting

Adherence to the correct procedures and safeguards, including the proper preparation and checking of warrants or authorisation records will reduce the scope for making errors. However, where a relevant error occurs, such as; activity taking place without a lawful authorisation or a failure to comply with the statutory safeguards, immediate steps must be taken to confirm the fact of an error expeditiously to C5 Crime Support Branch. Where it is subsequently confirmed as a relevant error, a full report will be provided to the Investigatory Powers Commissioner as soon as reasonably practicable.

A central repository will be retained of all errors reported and made available for inspections.

Appendix A – Contact Us

Branch e-mail

zC5CovertDataManagement