

NORTHERN IRELAND POLICING BOARD

NI POLICING BOARD RECORDS AND INFORMATION MANAGEMENT POLICY

RECORDS AND INFORMATION MANAGEMENT POLICY

Northern Ireland Policing Board

Version

Date of Version: September 2022

Review date: September 2026

Scope

- 1.1 This Records and Information Management Policy applies to the Northern Ireland Policing Board (the Board) records and information in all formats (electronic and physical files)². The policy aims to comply with the Lord Chancellor's Code of Practice on the management of records, issued under Section 46 of the Freedom of Information Act (2000). Moreover, the policy also aims to meet with the Board's strategic objectives by providing a foundation for good practice in the management of records and information assets to ensure the integrity of information held and helping ensure the Board delivers effective oversight of policing for the people of Northern Ireland.
- 1.2 This policy has been approved by the Senior Management Team (SMT). All staff must comply with this Records and Information Management Policy and related specific policies and procedures within its remit. All business functions and work undertaken must be documented fully as the Board records information and is kept as evidence and managed in compliance with this policy.
- 1.3 The Policy sets out the Board's best practice on how to manage all Board's records and information and covers:

Records and information in all formats – physical and electronic which includes records and information created by any system or technology (such as EDRM systems, Databases, Internets, Intranets, Email, Network drives, Physical Files etc).

Records and information throughout their life – from creation, use, management through to retention, transfer to archives or disposal.

² Board's Records applies to all records and information created, managed and stored in the Board. It sets a policy standard for the Directorates within the NIPB.

Records and information created or received from other organisations – physical and electronic records and information which has originated from another organisation when received or stored in any Board system or technology must be handled and managed in line with this Policy and any Information Security policies.

Records and information in any location – for example: in current use in offices; in filing cabinets; stored on servers; data transfers between the Board and outside Agencies created either internally or externally and stored in the Boards systems; remote and home working; records storage in-house or off-site; as well as any managed on behalf of the Board by an external body such as a contractor.

- 1.4 This Policy will be kept under review every 4 years and will be updated as appropriate strategies are agreed and implemented.

2. Introduction

- 2.1 Records and information constitutes a valuable asset for the Board and as such, is considered essential for the ongoing efficiency and effectiveness of business and for all staff to fully carry out their roles within the Board. Management of records and information as an asset will assist Board staff to deliver its key legislative duties.
- 2.2 Management of records and information delivered to Board customers via the Board's website and under Access to Information legislation must be accurate, impartial, timely, and available when required to support the public's access to the Board's information. There is also a statutory requirement to establish and maintain a FOI Publication Scheme on the Board's website outlining the functions of the Board and categories of information published in the course of delivering a public service.

- 2.3 Records and Information Management is a term used to describe an administrative system by which the Board seeks to control the creation, retrieval, storage, preservation or disposal of its records and information. Records and information is defined as: “recorded information, in any form, created or received and maintained by an organisation or person in the transaction of business or conduct of affairs and kept as evidence”. (ISO 15489-1:2016)
- 2.4 Effective management of records and information is essential to improve the efficiency and effectiveness of the Board and provide accountability for actions. The use and functionality of information systems are mechanisms to achieve the aims of this policy. Staff must have access to the right information when they need it to undertake their work.

3. Purpose of Policy

- 3.1 The purpose of this policy is to establish a framework for: ‘the creation and management of authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required...’ (ISO15489-1:2006).
- 3.2 The Board’s records and information management must meet the Public Records Act of Northern Ireland and related Statutory Orders, as well as a range of legislative requirements such as Freedom of Information, Environmental Information Regulations, Open Data, ECHR and Data Protection. In addition, the Board’s records and information should have sufficient evidential weight for legal admissibility in Judicial Inquiries, Court cases and other legal proceedings.

4. The Need for Records and Information Management

4.1 The Board's work depends totally on records and information and therefore this is one of our most important assets. The service that the Board delivers to its customers, whether internal or external, depends on efficiency in creating, using and storing information to make decisions and act in pursuit of corporate business objectives.

4.2 The Board aims that records and information:

- Can be identified and accessible to appropriate staff when required;
- Can be understood, fit for purpose and impartial;
- Can be trusted as evidence of business activities;
- Can be retrievable to comply with access to information statutory requirements;
- Can be managed over time and archived or appropriately destroyed; and
- Can be secured appropriately, depending on the protective marking.

4.3 This policy document outlines 7 key principles to ensure all staff:

- Treat records and information as a corporate resource across the organisation.
- Make sure the records and information they create, receive or capture are accessible to those who need it to fulfil their official duties.
- Manage all records and information, including information received or held on behalf of another organisations in a consistent manner across the organisation.
- Duty to document details of key business activities undertaken as part of official duties, as evidence of decisions and manage an audit trail of all policy decisions.
- Ensure all records and information are accurate, fit for purpose and useable.

- Take personal responsibility for the effective management of all records and information they create, use and store on the Board's systems (paper and electronic).
- Comply with all legislation, statutory requirements and standards to all records and information created, stored on the Board's systems, received and/or held on behalf of another organisation.

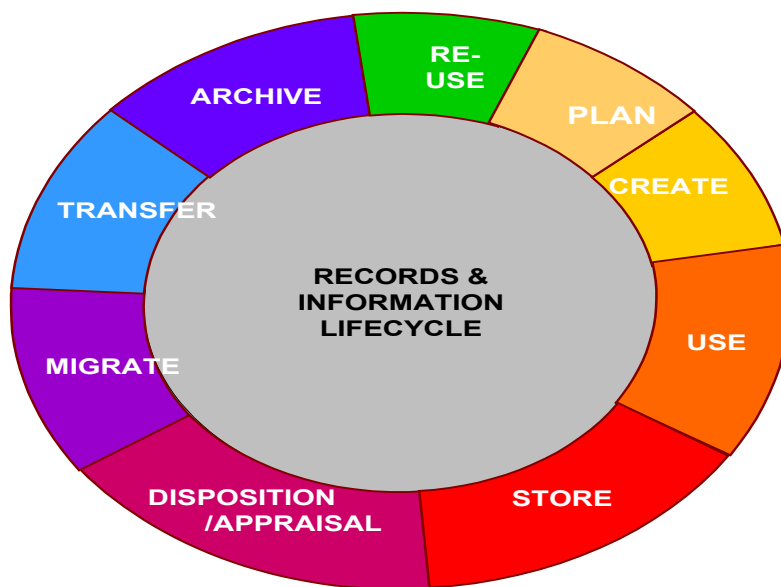
4.4 There are a number of pieces of legislation and standards which relate to effective management of all Board records, regardless of media or where it originated from (see Annex A). All records and information stored or held by Board staff in the course of normal business and on Board information systems, must comply with the legislation, standards and policies set out in this document. In addition, the Board is aware of the UK Government's influence on proposed legislation to open up government and provide more transparency and access to information.

4.5 Effective records and information management will not only meet legal requirements and standards but will enable the Board to:

- Access records when required, providing timely information for operational need
- Provide secure and legally admissible records demonstrating accountability
- Make better use of space and storage facilities both physically and electronically
- Optimise use of staff time and improve control over records, reducing costs
- Search and retrieve all relevant records and information held to comply with access to information requests
- Comply with best practice and other Board policies

4.6 It is vital that management of the Board's information resource is treated as an administrative discipline, which controls all aspects of the record life cycle, (see diagram 1 below), from record creation through to disposal, in an appropriate manner.

Diagram 1: Records Life Cycle



5. Aims and Objectives of Records and Information Management

5.1 The aim of this Records and Information Management Policy is twofold: firstly, to enhance delivery of services by ensuring the integrity of information and supporting timely and accurate records and information is retrievable when required, and secondly, to improve the quality of records – to create, use, maintain or dispose of the records in accordance with the Board's business need and legislative requirements and to ensure the permanent preservation of appropriately identified records.

The detailed objectives are to:

- Improve information retrieval methods by managing records and information which support the effective delivery of services and provide a reliable representation of business processes.
- Providing best practice guidance and professional advice on effective management of all Board records and information, which may be managed and stored on a variety of systems (electronic and physical) throughout the information Lifecycle.
- Ensure integrity of records and information by implementing policies and procedures to manage and store accurate and complete records which provide evidence of the rationale behind the decision-making processes as a public body and support auditing requirements.
- Provide support and mechanisms where appropriate to comply with Information Security standards and assist Information Asset Owner's responsibilities to manage information risks.
- Ensure compliance with access to information legislation and statutory deadlines. Maintain Information Asset Register and renewal as a data controller and ensure the Board has an up to date FOI Publication Scheme and Disclosure Logs in line with ICO guidelines. Improve records management of all information as well as the handling of personal data in line with Data Protection's principles and ICO's Data Sharing Code of Practice.

6. The Board's Statement of Commitment to Records and Information Management

6.1 The Board is committed to providing effective records and information management procedures and ensuring they are integrated as key activities within the organisation.

6.2 The Board will ensure creation, management, review and eventual archiving or disposal of records and information in a manner which accurately documents the functions of the organisation and is compliant with this policy.

- 6.3 The Board will ensure that the records and information management function supports the regulatory environment within which it operates as well as supporting access to delivery of services in a timely and accurate manner.
- 6.4 The Board will ensure that procedures, guidance and awareness are available to assist all staff in producing records which reliably represent accurate information that was used in or created by the business process and which will enable integrity and authenticity to be demonstrated.
- 6.5 The Board will ensure that all activities relating to records and information management from creation to disposal will be adequately resourced and supported. This will encompass records and information in all formats and will be organisation-wide.
- 6.6 The Board will implement processes and procedures to ensure timely compliance with access to information requests and statutory requirements such as FOI Publication Scheme and support Information Assurance and Information Security processes.

7. Responsibility for Records and Information Management

- 7.1 The implementation of this policy will be supported with range of guidance to staff to ensure the Board complies with all legislation related to records and information management.
- 7.2 The Chief Executive of the Board has overall responsibility for the organisational function of records and information management. Management and policy direction / guidance on records and information management is delegated to the Communications Manager. On Privacy and Data Protection Act, the Data Protection Officer is the key contact.

- 7.3 The Records Management Team is the key point of contact within the Board on all records and information management and personal data activities. Compliance monitoring with Public Records Act and Access to Information legislation are principle parts of these roles. This team co-ordinates the provision of advice and guidance related to this Records and Information Management Policy throughout the Board.
- 7.4 The Chief Executive of the Board also has overall responsibility as the Board's Senior Information Risk Owner (SIRO). The Board's Information Asset Owners (IAOs) have been identified as the Board's Directors. The SIRO will report to IROC³ on any information risks and security issues.
- 7.5 The Board's Security Officer (Director of Resources) is the key point of contact on all information security issues and for ensuring that all Board information is appropriately protected.
- 7.6 All information security incidents should be dealt with in accordance the Security Incident Reporting Policy (Record No. 368179).
- 7.7 Staff are appointed within each Directorate to review records, they will be co-ordinated by the Records Management Team who are the first point of contact on all records and information management queries and issues. The Records Management Team will provide advice and guidance and implement processes to meet business requirements in line with this policy.
- 7.8 All staff in the Board are under a statutory obligation to create accurate records of their activities, document decision making and to manage such documentation. Staff are responsible for:
- Identifying records and information which should be captured because of their business function or content.
 - Creating records which are consistent, reliable, accurate and complete.

³ Information Risk Owners Council (IROC) is a key component of the Department of Justice's (DOJ) structure for information risk management

- Capturing records which authentically document activities and decision making in the course of which they were produced.
- Filing and storing records and information in the appropriate area of the Corporate Fileplan within the EDRMS or in line of business systems. Physical files should be discontinued wherever possible and digital systems adopted or utilised better.
- Ensuring they have a clear understanding of this Records and Information Management Policy and demonstrating commitment to duties relating to their own record keeping.
- Awareness of information security and access controls and how they apply to records and information where appropriate.
- Awareness of appropriate retention and disposal periods for records and information.
- Responding to access to information requests within the Board's targets and statutory deadlines and assessing records and information which may be released to comply with this legislation.
- Handle and process personal information in line with Data Protection Act's principles, ICO's Data Sharing Code of Practice and use appropriate protective markings as required.

8. Security of Records and Information

- 8.1 Protective markings should be assigned to all records and information in line with policies and guidance issued by the Records Management Team. All Information systems are accredited and as part of this it is determined what the maximum level of security can be afforded to the records and information managed and stored within. Whenever using any information system, staff should be aware of the maximum security level that applies and protectively mark relevant records and information as required.
- 8.2 Electronic records and information on the Board's network are classified as Official but may take categories especially 'Official-Sensitive' to protect personal data. Records and information classified as 'Secret' may be created

and maintained on an accredited separate network (if the business area has access to this) and / or on registered physical files; as long as they are registered on an Information Asset Register and stored and protected in line with their protective marking.

- 8.3 All staff have a duty to protect records and information for which they are responsible, even though it is to be shared within legal constraints for business purposes and made as widely accessible as possible.
- 8.4 Records and Information Management procedures will be developed to maintain appropriate audit trails on the use of records and information and ensure access controls are managed.

9. Retention and Disposal of Records and Information

- 9.1 The Records Management Team will provide advice and guidance on the principles of Retention and Disposal Schedules. The Board will use and maintain a Retention and Disposal Schedule for all records and information to meet Public Records Act of Northern Ireland requirements.
- 9.2 A Retention and Disposal Schedule is a key tool and mechanism in the management of records and information and outline all classes of records and how long they are needed for business reasons or to comply with regulatory obligations. The Schedule will also clearly document the final action, which will after appraisal processes have been undertaken, result in authorised destruction of records and information or transfer to an archive.
- 9.3 The Retention and Disposal Schedule is legally required to be signed off by the NIPB Chief Executive, NIPB Communications Manager, PRONI's Deputy Keeper of the Records, PRONI's Head of Records Management, Cataloguing and Access Team and DCAL's Permanent Secretary as the Head of the Department with responsibility for PRONI. A Retention and Disposal Schedule

that has been signed off is laid at the Northern Ireland Assembly by PRONI on behalf of the Department of Communities Minister as Keeper of the Records.

- 9.4 The Records Management Team provides guidance on retention and disposal actions for records and information relating to common functions, such as Financial or HR Management etc. Retention and disposal actions for records and information relating to each Directorate's specific functions will be developed by the relevant Directorate, while the Records Management Team will be available to quality review the schedule to ensure consistency in approach is adopted.
- 9.5 Procedures for implementing retention and disposal scheduling actions for all records and information have been developed and Information Asset Owners are notified. Directorates will be responsible for implementing retention and disposal scheduling actions as part of their own records and information management activities and informing the Records Management Team of actions taken in Disposal logs.
- 9.6 Once records are selected for destruction in accordance with the schedule and any guidelines, the method of disposal should be appropriate to any security markings and should be done in a secure manner and be fully documented in line with the Board's Retention and Disposal Schedule.
- 9.7 Where a record due for destruction becomes the subject of a request for information, court case or an Inquiry, this will be delayed by a 'legal hold' and the Board's Retention and Disposal Schedule updated until the request or legal proceedings have been closed or, in the case of a refusal/appeal, until the appropriate time limit has expired or been exhausted.

10 Historical Records

- 10.1 Historical records are those deemed to have permanent archival value for legal, administrative or research purposes. These records will be identified on the approved Retention and Disposal Schedule and managed by the Board in consultation with PRONI.
- 10.2 Archiving of any Information system and / or the records and information they contain will take into consideration the management of personal data for as long as it is required and the agreed retention / disposal actions to be applied.
- 10.3 Digital Continuity issues will be taken into consideration during the application of retention and disposal scheduling to ensure long term accessibility to records and information for legal and regulatory reasons on systems and networks.

11. Other NI Policing Board policies and procedures

- 11.1 This document is the Board's overarching Records and Information Management Policy, which outlines requirements at a high-level and is part of a framework of policies to be issued across the organisation. Below this policy lies a range of other policy guides on more specific topics and which provide all staff with more detailed guidance as required. A list of published information, policy guides and other policies relevant to this area are provided at Annex B.

12 Contacts

Further Contact Information
For records management or access to information (FOI / DPA) queries contact the Records Management Team

Annex A –

Associated legislation and standards

The following is a list of current external legislation and standards which are particularly relevant to this policy. Please note this is not an exhaustive list of all records and information related legislation or standards.

- Public Records Act (NI) 1923 and Disposal of Documents Order (NI) 1925
- Freedom of Information Act 2000
- Data Protection Act 1998
- Environmental Information Regulations 2004
- Section 46, Freedom of Information Act 2000 – known as the Lord Chancellor’s Code of Practice on the management of records
- Information Commissioner Office (ICO) Data Sharing Code of Practice
- ISO 15489-1:2001 Information and Documentation – Records Management and ISO 15489-2:2001 Guidelines for Implementation, can be ordered from British Standards Organisation
- BS BIP 0025-1: 2002 Effective records management. Management guide to the value of BS ISO 15489-1; BS BIP 0025-2: 2002 Effective records management. Practical Implementation of BS ISO 15489-1; BS BIP 0025-3: 2003 Effective records management. Performance management for BS ISO 15489-1; BS BIP 0025-4: 2007 Effective records management, How to comply with BS ISO 15489-1
- BS ISO 23081:2006 Information and documentation, records management processes metadata for records
- ISO/IEC 27001:2005 (formerly BS 7799-2:2002) Specification for Information Security
- ISO BS 10008:2008 Evidential weight and legal admissibility of electronic information
- BS 4783-4:1988 Storage, transportation and maintenance of media for use in data processing and information storage
- BS 10012:2009 Data protection, specification for a personal information management system
- BS PD 0010:1997 The principles of good practice for information management
- Northern Ireland Records Management Standard can be viewed on the Public Record Office of Northern Ireland website at: www.proni.gov.uk

Annex B – NI Policing Board policies and procedures

The Following Policies are relevant to the Board's Records and Information Management Policy: -

- Data Protection Policy
- Data Protection Impact Assessment Policy
- Freedom of information Policy
- Retention and Disposal Schedule
- Retention and Disposal Policy
- NIPB Information Security Policy
- Records Management Policy Statement

Ongoing Support and Advice

1. For further information on records management and the Board's Retention and Disposal Scheduling support the Records Management Team can be contacted at:

- Internal extension 83528 or
- FOI@nipolicingboard.org.uk

2. Further advice and guidance is also available at:

- For NICS-wide policies and guidance on managing information, see <http://nics.intranet.nigov.net/staff-services/nicsmi>

 028 9040 8500

 information@nipolicingboard.org.uk

 www.nipolicingboard.org.uk

 [policingboard](https://www.facebook.com/policingboard)

 [@nipolicingboard](https://twitter.com/nipolicingboard)

 [nipolicingboard](https://www.youtube.com/nipolicingboard)

 [Northernirelandpolicingboard](https://www.linkedin.com/company/northernirelandpolicingboard)

DOCUMENT TITLE

**NI Policing Board Records and
Information Management Policy**

DISCLAIMER

While every effort has been made to ensure the accuracy of the information contained in this document, the Northern Ireland Policing Board will not be held liable for any inaccuracies that may be contained within.