The Regulation and Quality Improvement Authority

HSC Business Services Organisation

Information Governance Policy

Title:	Information Governance Policy		
Ownership:	Information Governance Group		
Approved by:	RQIA Policy Group RQIA EMT BARC Authority	Date Approved:	9 October 2025 14 October 2025 6 November 2025 11 December 2025
Date Implemented		Date for Review:	01.04.2028
Version No.	3.1	Supersedes:	v3.0
Director Responsible	Chair of Information Governance Group		
Key Words:	Information Governance, Data Protection, Information Security, Freedom of Information, Data Breach, Personal Data, Records Management		
Links to other Policies, Procedures & Guidance	Data Protection and Confidentiality Policy		
	Freedom of Information Policy		
	Records Management Policy		
	Information Security Policy		
	Incident Reporting Policy		

Table of Contents

1 Introduction

1.1 Information governance (IG) describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information are processed appropriately, securely and in line with current legislation. It has four fundamental aims:

- to support the provision of a high-quality service by promoting the effective and appropriate use of information
- to encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources
- to provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards
- to enable organisations to understand their own performance and manage improvement in a systematic and effective way

1.2 Information held by RQIA represents one of their most valuable assets, and core to most of the services delivered.. It is therefore essential that all information is managed effectively within a robust framework, in accordance with best practice and legislative and policy requirements, as set out within the RQIA's and BSO's Information Governance Assurance Framework.

1.3 Having accurate relevant information available at the time and place where it is needed, is critical in all areas of business and plays a key part in corporate governance as well as risk, planning and performance management.

1.4 The RQIA carries a legal responsibility for the appropriate processing and protecting information of many types. This includes information which contains personal details of patients/clients, their families or staff.

1.5 This policy also recognises the necessity to share some personal data with other health organisations and agencies in a controlled manner consistent with the interests of the individual and, in some circumstances, in the public interest.

1.6 Some information may be non-confidential and is for the benefit of the general public. Examples include information about services, annual report and business plans. The RQIA and its staff share responsibility for ensuring that this type of information is accurate, up to date and easily accessible to the public.

1.7 Although the majority of information about RQIA should be open for public scrutiny, it is acknowledged that some information will need to be safeguarded. Examples include, but are not restricted to:

- Information that would be considered a breach of data protection requirements should it be released
- Information considered commercially sensitive
- Information provided in confidence
- Information covered by legal professional privilege

2 Purpose

2.1 The IG requirements set out within this policy and other policies and procedures are intended to:

- outline the approach to fulfilling IG responsibilities;

- ensure compliance with legal and regulatory framework is maintained;
- establish a robust framework for preserving the confidentiality, integrity, security and accessibility of data, systems and information;
- give assurance that information is processed legally, securely, efficiently and effectively

2.2 The IG requirements set out within this policy and other policies and procedures are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used and ensuring that relevant information is available where and when it is needed.

3 Scope

3.1 The scope of this policy is to support the protection, control and management of information and information assets. The policy will cover all information held by, or on behalf of, RQIA and is concerned with all information systems, electronic and non-electronic, as well as all records whether held electronically or manually. It applies to all directorates, services and departments, all staff, and as appropriate to contractors and third party service providers acting on behalf of RQIA.

3.2 IG covers all information held, and all information systems purchased, developed and managed by/or on behalf of, the BSO and RQIA and any individual directly employed or otherwise used by the RQIA to hold that information on any media, and in any format.

.

3.3 This policy covers all forms of information held, including personal identifiable data as defined in data protection legislation, as well as non-personal identifiable data (such as organisational, business and operational information).

4 Policy Statement

4.1 Openness: RQIA will:

- establish procedures and arrangements for handling requests from service users and members of the public under provisions of Freedom of Information and Subject Access Requests
- undertake regular assessments of IG policies and arrangements
- ensure that publicly disclosable information about the organisation and its services is readily and easily available, in line with the Freedom of Information Act 2000, Environmental Information Regulations 2004 and the Information Commissioner's Office's (ICO's) model publication scheme
- ensure that privacy notices are published to advise the public according to its obligations under the UK GDPR, including:
    - the purposes of the processing of personal data
    - legal basis for the processing
    - categories of personal data processed
    - the recipients or categories of recipients of the personal data
    - retention periods of personal data
    - the rights of data subjects, including the right to contact the ICO

4.2 Legal Compliance: The RQIA will:

- establish and maintain policies and procedures to ensure compliance with data protection legislation, the common law duty of confidentiality, Environmental Information Regulations 2004, and the Freedom of Information Act 2000
- develop and maintain the appropriate registers and systems to permit its functions as a data controller where this is required
- develop and provide sufficient guarantees in its capacity as a processor as to appropriate technical and organisation measures for the services it provides to the wider HSC
- establish and maintain policies and procedures for the controlled and appropriate sharing of personal data, taking account of relevant legislation

4.3 Information Security: RQIA is dedicated to the secure management and use of information held, and will ensure information security is embedded into relevant policies and procedures, including:

- , establish and maintain appropriate incident reporting procedures to report, monitor and investigate all instances actual and/or potential along with any reported breaches of confidentiality and security
- undertake and/or commission audits to assess Information and ICT Security arrangements
- promote effective confidentiality and security practice to ensure all staff and third-party associates adhere to this policy, and associated policies and procedures

4.4 Information Quality Assurance: Information quality is fundamental to supporting business decision making processes. The RQIA will ensure that information they hold is of the highest quality, and will:

- establish and maintain appropriate policies and/or procedures for information quality assurance
- undertake or commission regular assessments and audits of its information quality and records management arrangements
- ensure that data standards are set through clear and consistent definition of data items, in accordance with quality standards
- promote information quality and effective records management through policies, staff awareness and training
- report and act upon incidences of known or suspected poor data quality

4.5 Information Risk Management: The RQIA will:

- risk assess all information assets and information flows to determine that appropriate, effective and affordable IG controls are in place
- put in place appropriate contingencies to reduce risk to an accepted level, where appropriate

4.6 Records Management: The underlying principle of records management is to ensure that a record is managed through its life cycle from creation or receipt, through maintenance and use to disposal. The RQIA will:

- establish and maintain a policy and appropriate procedures for effective records management
- promote records management through policies, procedures and training
- adhere to the regional retention schedule (‘Good Management, Good Records’ - GMGR)

4.7 Training: The RQIA will ensure that:

- training is assessed for quality, and specific training is available for different roles as appropriate
- all staff complete mandatory training at induction, and on a 3 yearly cycle thereafter
- all staff have access to relevant IG policies and procedures

5 Roles and Responsibilities

5.1 Responsibilities are as set out within BSO and RQIA's Information Governance Assurance Framework (IGAF), which is available on request.

5.2 RQIA will also operate an internal Information Governance Group (IGG), with representation from each service area. The role of this group is set out within the the RQIA Controls Assurance.

6 Performance and Monitoring Compliance

Monitoring of performance is set out within subsequent policies, namely:

- Data Protection and Confidentiality Policy
- Freedom of Information Policy
- Records Management Policy

7 Non-Compliance

(1) A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action.

In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law.

(2) Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

8 Review

This policy shall be reviewed regularly, and as a minimum:

- every 3 years; or
- following receipt of new information; or
- following updates to applicable legislation, guidance or best practice; or
- upon implementation of new agreements which may affect the policy

9 Equality Statement

This policy has been screened for equality implications as required by Section 75 of the Northern Ireland Act 1998 and it was found that there were no negative impacts on any grouping. This policy will therefore not be subject to an Equality Impact assessment.

Information Governance Assurance Framework

Title:	Information Governance Assurance Framework		
Ownership:	Information Governance Group		
Approved by:	Policy Group EMT BARC Authority	**Date Approved:**	9 October 2025 14 October 2025 6 November 2025 11 December 2025
Date Implemented:		**Date for Review:**	01.04.2028
Version No.	3.2	**Supersedes**	3.0
Director Responsible:	Chair of Information Governance Group		
Key Words:	Information Governance, Data Protection, Information Security, Freedom of Information, Data Breach, Personal Data, Records Management		
Links to other Policies, Procedures & Guidance	Data Protection and Confidentiality Policy Freedom of Information Policy Information Governance Policy Information Security Policy Incident Reporting Policy		

Contents

1. Introduction

1.1 Information governance (IG) is the framework of legislation, policy and best practice guidance that regulates the manner in which information (including information relating to and identifying individuals) is managed, i.e. obtained, handled, used and disclosed.

1.2 The Information Governance Assurance Framework (the "Framework") is a framework that bring together all statutory, mandatory and best practice requirements concerning information management. The requirements are set out in the Department of Health (DoH) Information Management Assurance Checklist (IMAC) as a road map enabling the Business Services Organisation (BSO) and RQIA to plan and implement standards of practice and to measure and report compliance on an annual basis.

1.3 BSO performance against the IMAC is mandated by and reported to the DoH and forms part of BSO's annual assurance processes.

1.4 This document sets out an overarching framework for the IG agenda in the BSO and RQIA. In particular, this framework looks at the operational and management structures, roles, responsibilities, systems, policies and audit controls that are used to ensure such issues are appropriately addressed throughout BSO and RQIA. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

1.5 This policy also acts as an overall umbrella policy that sets out the approach to be adopted for the processing of information, sitting over the other policies relating to each aspect of IG.

1.6 This Framework document sets out requirements to support assurance against the IMAC.

2. General principles

2.1 IG is about the way in which RQIA handles its information, particularly personal information. RQIA relies on good quality information being available at the point of need in order to provide a high quality service. Staff rely on the quality of information they use to make decisions and the way in which they use resources and run RQIA's business. It is important for staff to understand their own responsibility for recording information to a consistently high standard and for keeping it secure and confidential where required to. Public confidence inRQIA's ability to handle information, including personal information responsibly and efficiently is based on a good reputation for keeping information safe.

2.2 Reference to information governance, in this document shall also mean reference to the following areas:

- Freedom of Information Legislation
- Environmental Information Legislation
- Data Protection Legislation
- Information security assurance

- Information quality assurance
- Information risk management
- Records Management.

2.3 Information Governance provides a consistent way for staff to deal with the many different information handling requirements. Listed below are the legislation, policy, standards, guidelines, and best practice guidance applicable to this Framework:

- The Data Protection Act 2018
- UK General Data Protection Regulation
- The Access to Health Records (Northern Ireland) 1993
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The Common Law Duty of Confidentiality
- The Caldicott Guardian Manual 2010
- The Human Rights Act 1998
- Section 75 (NI Act 1998)
- The Public Records Act (Northern Ireland) 1923
- The Disposal of Documents Order 1925
- The Re-use of Public Sector Information Regulations 2015
- The Electronic Communications Act 2000
- The Public Interest Disclosure Act 1998
- The Computer Misuse Act 1990
- The Crime and Disorder Act 1998
- The Investigatory Powers Act 2016
- Department of Health (DoH) Good Management Good Records (GMGR)
- Health and Social Care (HSC) Code of Conduct
- DoH Code of Practice on Protecting the Confidentiality of Service User Information
- DoH Information Management Assurance Checklist (IMAC)
- Guidance from the Information Commissioner's Office (ICO)

2.4 A suite of policies, in line with the above, will be produced under this Framework. As a minimum these will include:

- IG Policy
- Freedom of Information Policy
- Data Protection and Confidentiality Policy
- Records Management Policy

2.5 This Framework and suite of policies should also be read in conjunction with relevant BSO and RQIA ICT policies.

3. Annual IG Assurance

3.1 BSO's and RQIA's compliance against the IMAC is completed by its Data Protection Officer (DPO), with assurance thereafter provided to DoH by the BSO's SIRO or CEO.

3.2 BSO for RQIA will seek to maintain compliance with the IMAC on a yearly basis.

5. Information Governance Training

5.1 Fundamental to the success of delivering the Framework is developing an IG culture within RQIA. Basic awareness and training will be available to all RQIA staff either via face-to-face training or an e-learning package.

5.2 IG Training is incorporated into RQIA Mandatory Training programme. It is a **mandatory** requirement for all staff in RQIA, without exception, to undertake IG training once every two years.

5.3 Different levels of training will be delivered:

- All staff will receive Information Governance awareness training as part of their corporate induction programme.
- Internal training for staff who handle personal data as a routine part of their job will be available via the Data Protection Officer (DPO), and
- Additional training will be provided for those engaged in, or intended to take on IG specialist roles e.g. SIRO (Senior Information Risk Owner), Personal Data Guardian (PDG) and Information Asset Owners (IAOs)

6. Communications Plan

6.1 RQIA relies upon BSO to develop and maintain communications (i.e. privacy notices) to ensure that all stakeholders are adequately informed about

- the identity of RQIA and its Data Protection Officer (DPO);
- RQIA data BSO processes personal data on behalf of, and which organisations receive this personal data;
- the purpose(s) for processing of personal data and the lawful basis;
- the categories of personal data processed; and
- the rights of all stakeholders in line with data protection legislation

6.2 BSO and RQIA will develop and issue communications specific to staff, to remind them of specific responsibilities.

7. Roles and Responsibilities

7.1 These definitions in this section apply to all IG policies that sit as part of this framework

7.2 The ARAC **Governance and Audit Committee** of RQIA's Authority has overall responsibility to oversee the establishment and maintenance of an effective system of internal control, including the adequacy of this framework and related policies.

7.3 The **Chief Executive, as the accountable officer,** has responsibility for maintaining a sound system of internal governance that supports the achievement of the Organisation's policies, aims and objectives.

7.4 The **Personal Data Guardian (PDG)** is a senior person within RQIA who is

responsible for ensuring that that the personal data about those who use the organisation's services is used legally, ethically and appropriately, and that confidentiality is maintained. The PDG Chairs the RQIA Information Governance Committee.

7.5 The **Senior Information Risk Officer (SIRO)** takes overall ownership of the Organisation's Information Risk Policy, act as champion for information risk and provide written advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control in regard to information risk.

7.6 **Information Asset Owners** (**IAOs)** are senior individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide written input to the SIRO on the security and use of their asset.

7.7 The IAO is responsible for ensuring that information and assets associated with information processing facilities are appropriately identified and classified; including defining and periodically reviewing access restrictions, classifications, and business continuity arrangements taking into account applicable access control policies. Routine tasks may be delegated, e.g. to a member of staff using the asset in the discharge of their duties, but the responsibility remains with the IAO.

7.8 In line with Article 39 of the UK GDPR, the **Data Protection Officer (DPO)** shall have at least the following tasks:

- to inform and advise RQIA and its staff of their obligations pursuant to data protection legislation
- to monitor compliance with data protection legislation and this framework in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to cooperate with the ICO;
- to act as the contact point for the ICO on issues relating to processing

7.9 In addition, the DPO (or an appropriate delegate) will also be responsible for:

- ensuring there is senior level awareness and support for IG
- reviewing this Framework and associated policies
- developing appropriate training for staff across the suite of IG

7.10 **Managers and supervisors** are responsible for implementing this framework within their team structure.

7.11 **All staff** are responsible for familiarising themselves with, and adhering to, all parts of this framework.

7.12 Any **third parties** who process information for or on behalf of the RQIA and BSO will be required to confirm and demonstrate that they will abide by the requirements

of data protection legislation and this framework.

7.13 The RQIA operates an internal group **Information Governance Group (IGG)**, with representation from each service area. As per its terms of reference, the role of IGMG will be:

- To ensure that RQIA has effective policies and management arrangements covering all aspects of IG in line with legislation and best practice
- To provide a forum to raise awareness and share experience and best practice in relation to IG
- To ensure that RQIA undertakes self-assessments and/or audits of IG policies and arrangements.
- To establish and approve improvement plans where necessary, and monitor and review the implementation of these plans.
- To review breaches of data protection, and where appropriate implement remedial action and/or disseminate 'lessons learnt' within RQIA
- To liaise with other RQIA staff within individual teams / directorates, in order to promote IG issues.

8. Information Risk

8.1 RQIA's overall approach to risk will apply in to all of its processing of information, namely: "The RQIA will ensure that the management of risk is an integral element of its work in relation to customers, staff and the public (where relevant)"

8.2 IAOs will provide assurances to the SIRO on the security and use of assets where they have been assigned 'ownership' of. This should include a risk assessment, including (where applicable) an assessment of forthcoming potential changes in services, technology and threats.

8.3 Further information on the management of information risk is available in the **Information Governance Policy**.

8.4 All appropriate risks will be entered onto the appropriate service risk register as documented in RQIA's **Risk Management Strategy**. Further to this any severe risks will be reported to EMT for consideration and possible inclusion on the Corporate Risk Register.

8.5 The SIRO will be made aware of all information risk assessments and approve any identified risk mitigation plans.

9. Information Security Incident Management

9.1 The PDG and SIRO must be informed immediately of all information security incidents involving the unauthorised disclosure of person identifiable data/information for consideration of any necessary actions.

9.2 The PDG and SIRO will inform the DPO who in turn will disseminate significant security breaches to the SIRO and ICO as deemed necessary.

9.3 A key function of the IGG is to monitor and review untoward occurrences and

incidents relating to IG and to ensure that effective remedial and preventative action is taken. Reports of such incidents will be distributed to the IGG for consideration.

9.4 Information incident reporting will be in line with RQIA's overall incident reporting processes. Please refer to the **Adverse Incident Reporting Policy**.

10. Security of Information

10.1 RQIA will protect all information it holds, regardless of type and format held through compliance with the legislation, policy, standards, guidelines, and best practice guidance as set out in Section 2.3 of this Framework.

10.2 Please refer to the **Information Security Policy** and **Data Protection and Confidentiality Policy** for more detailed guidance on encryption and access to service user information.

11. Data Protection Impact Assessments (DPIAs)

11.1 The impact of any proposed changes to the processes and/or information assets need to be assessed in accordance with the RQIA's Risk Management Strategy and the RQIA IG Policy, to ensure that the confidentiality, integrity and accessibility of personal data are maintained.

11.2 The DPO should be consulted during the completion of any DPIA, in order that they can provide appropriate advice.

11.3 Please refer to the **Data Protection and Confidentiality Policy** for more detailed guidance on completion of DPIAs.

12. Information Asset Register (IAR)

12.1 All assets should be clearly identified in each service area and a register of all assets maintained across RQIA.

12.2 It will be the responsibility of each IAO to identify what information assets are held within their area of responsibility, and to ensure this is documented in the IAR.

12.3 The IAR should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information and license information. Ownership should be agreed and documented for each of the assets.

12.4 Based on business criticality of the asset, and its security classification, commensurate levels of protection should be identified as should details of risk assessment.

12.5 All information assets should be assigned to designated part of RQIA, e.g. a business unit.

12.6 In complex information systems it may be useful to designate groups of assets, which act together to provide a particular function as 'services'. In this case the

service owner is responsible for the delivery of the service, including the functioning of the assets, which provide it.

13. Freedom of Information and Environmental Information

13.1 RQIA will ensure compliance with the Freedom of Information Act 2000 and ICO guidance. This is set out in RQIA's Freedom of Information and Environmental Information Policy.

14. Confidentiality of Personal Data

14.1 RQIA will ensure that all personal data it holds is managed in accordance with data protection legislation. This is set out in BSO's **Data Protection & Confidentiality Policy**

15. Records Management

15.1 RQIA is committed to a systematic and planned approach to the management of records from their creation to their ultimate disposal. RQIA will ensure that it controls the quality and quantity of the information that it generates, can maintain that information in an effective manner and can dispose of the information efficiently when it is no longer required. This is set out in the Records Management Policy. It is also set out in the GMGR

15.2 To ensure that RQIA maintains the highest standards in the quality of its records an annual self-assessment of corporate records will be undertaken. This will be completed via IGG.

16. Third Party Contracts

16.1 It is not unusual to have third parties gaining access to information assets, e.g. computers, telephones, paper records etc. It is possible that as a result of access to information assets, third party staff may have significant access to personal/ sensitive personal data. This situation therefore clearly has information governance risk implications such as data being used inappropriately.

16.2 Suitable clauses must be included in contracts with third parties who have access to or process personal data on behalf of RQIA, in line with requirements within data protection and any other applicable legislation.

16.3 In line with Article 28 of UK GDPR, contractors must be made aware, via contract clauses, that they cannot engage with another processor without prior specific or general written authorisation from RQIA. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

16.4 The SIRO and IAOs must take all reasonable steps to ensure that third parties to whom personal data is disclosed comply with their contractual obligations to keep personal data secure and confidential.

16.5 Directorates and IAOs should ensure that a risk assessment has been carried out prior to any agreement being made with a third party to evaluate any potential threats to networks, systems and locations from third party operatives. The ways in which third parties gain access, will help determine how extensive the risk assessment needs to be. For example, a risk assessment for cleaning contractors will be different to that carried out for a contractor connecting to the network. Temporary access will also see different considerations to long-term access.

16.6 IAOs should ensure that all existing contracts are monitored and reviewed annually to ensure that IG controls are being adhered to and to resolve problems or unforeseen events.

16.7 A register of all third-party contracts should be maintained.

17. Information Sharing with other HSC Organisations

17.1 Sharing information with other HSC organisations is vital to the provision of co-ordinated and seamless services within HSC. However, the need for robust documentation of this sharing is recognised.

17.2 Such sharing requires the use of an agreed format template (such as a data access agreement) in order to ensure that the requirements of law, policy and guidance are being met.

18. Information Quality Assurance

18.1 The quality of information acquired and used within RQIA is a key component to its effective use and management. As such, managers will be expected to take ownership of, and assure, the quality of data collected and held.

18.2 Information and data quality will be promoted through the use of policies and training of staff to ensure that wherever possible, information quality will be assured at the point of collection.

19. Information Governance Improvement Plans

19.1 An essential element of the IGG is that RQIA continues to monitor and, where appropriate, improve performance in relation to IGG. This will be done via completion of an annual self-assessment against the IGG.

19.2 In order to achieve this, IGG will develop a rolling annual action plan in Q4 of each year, based on the most recent IMAC self-assessment and known events programmed for the future audit recommendations and IGG knowledge of RQIA's IG issues This plan will be used to determine the course of IG activity for the forthcoming year and should contain the following clearly defined areas:

- SMART objectives and deliverables
- Resources required
- Ownership assigned
- Identified IG risks that may impact upon delivery of the plan

19.3 The plan will be refreshed as required in year in response to non-forecasted events.

20. Review and Monitoring

20.1 This framework will be reviewed every three years by IGG to ensure compliance with legislation and the requirements of the IMAC. Recommendations for amendment will be reported to the SIRO.

21. Equality Statement

21.1 This policy has been screened for equality implications as required by Section 75 of the Northern Ireland Act 1998 and it was found that there were no negative impacts on any grouping. This policy will therefore not be subject to an Equality Impact assessment.

Data Protection and Confidentiality Policy

Title:	RQIA Data Protection and Confidentiality Policy		
Ownership:	Information Governance Group		
Approved by:	Policy Group EMT BARC Authority	Date Approved:	9 October 2025 14 October 2025 6 November 2025 11 December 2025
Date Implemented:		Date for Review:	01.04.2028
Version No.	2.2	Supersedes:	v.2.0
Director Responsible:	Chair of Information Governance		
Key Words:	Data Protection, Confidentiality, Responsibility		
Links to other Policies, Procedures & Guidance:	Information Governance Policy		
	Information Security Policy		
	Records Management Policy		
	Policy for the reporting of adverse incidents, accidents, near misses and dangerous occurrences		
	Freedom of Information and Environmental Information Policy		

Contents

1. Introduction

1.1 (RQIA) needs to process personal data[1] about data subjects in order to carry out its business, provide its services and otherwise for or in connection with its statutory functions. Such data subjects include but are not limited to patients, staff (present, past and prospective), suppliers and other business contacts. In addition, RQIA may be required by law to process and share personal data with other organisations (including, but not limited to, police, regulatory and other health and social care bodies).

1.2 As a public body, RQIA has a statutory duty to safeguard the personal data it holds, from whatever source. The lawful and proper treatment of personal data by RQIA is extremely important to the success of RQIA's business and in order to maintain the confidence of RQIA's service users and employees.

1.3 A failure to comply with data protection obligations may expose RQIA to substantial fines and/or liabilities, as well as reputational damage.

1.4 It is therefore important that personal data is managed effectively within a robust framework, in accordance with best practice and legislative and policy requirements, as set out within RQIA's and BSO's Information Governance Assurance Framework.

2. Purpose

2.1 The purpose of this policy is to support the protection, control and management of personal data. The policy will cover all personal data processed by or on behalf of RQIA, regardless of the media on which that data is stored or transmitted, or the data subject(s) to which is relates. It applies to all directorates, services and departments, all staff, and as applicable to contractors and third party service providers acting on behalf of RQIA.

2.2 This policy has been written to support staff in compliance with legislation, policy and best practice guidance relating to the protection of personal data, as set out within BSO and RQIA's Information Governance Assurance Framework

3. Scope

3.1 The following definitions are as defined within Articles 4 and 9 of the UK GDPR.

- 'personal data' means any information relating to an identified or identifiable natural person[2] ('data subject');
- 'special categories' of personal data is personal data relating to one or more of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, health (mental or physical), sexual life or sexual orientation[3];
- 'data controller' is the natural or legal person, public authority, agency or

[1] Personal data has the meaning as set out in Section 4 of this policy

[2] An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

[3] For the purpose of this policy, the terms 'personal data' and 'special category of personal data' will both be referred to as 'personal data', unless otherwise stated

any other body which alone or jointly with others determines the purposes and means of the processing of personal data

- 'data processor' is a natural or legal person, public authority, agency or any other body which processes personal information on behalf of the data controller;
- 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
- 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

4. Roles and Responsibilities

4.1 Roles and responsibilities are as set out within BSO's and RQIA's Information Governance Assurance Framework

Personal data

5. Data Protection Principles and Data Protection by Design

5.1 RQIA, its staff and others who process personal data on its behalf must ensure that they follow the principles set out within Article 5 of the UK GDPR, namely that personal data will be:

- processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5.2 In addition, the UK GDPR requires RQIA to implement appropriate technical and organisational measures to implement the above principles and safeguard individual rights. This is known as 'privacy by design and by default'.

5.3 Requirements for this are set out within subsequent sections of this policy.

6. Lawfulness, Fairness and Transparency

6.1 RQIA will only process personal data if doing so satisfies one or more of the criteria as set out within Article 6, and where applicable, Article 9 and Article 10 of the UK GDPR and associated provisions of the Data Protection Act 2018.

6.2 The lawful basis for the processing of personal data, as set out in Article 6 UK GDPR, are as follows:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal/statutory obligation to which the controller is subject to;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (although 'legitimate interest cannot generally be used by public bodies as a basis for processing, it is included here in the interest of completeness).

6.3 RQIA will only process special categories of personal data where one or more lawful basis has been identified. The lawful basis for the processing of special

category personal data, as set out in Article 9 of UK GDPR, are as follows:

- the data subject has given explicit consent;
- the processing is necessary in the context of employment law, or laws relating to social security and social protection;
- the processing is necessary to protect vital interests of the data subject or of another natural person;
- the processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes;
- the processing relates to personal data which have been manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity;
- the processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects the rights of data subjects;
- the processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and services;
- the processing is necessary for reasons of public interest in the area of public health (e.g. ensuring the safety of medicinal products);
- the processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.

6.4 In accordance with Article 10 of the UK GDPR, RQIA will only process personal data relating to criminal convictions and offences or related security measures under the control of official authority or when the processing is authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects

6.5 In line with guidance from the ICO, 'lawfulness' will also mean that RQIA must not process personal data that is unlawful in a more general sense. If processing involves committing a criminal offence, it will be unlawful. However, processing may also be unlawful if it results in:

- a breach of a duty of confidence;
- your organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations; or
- a breach of the Human Rights Act 1998

6.6 The RQIA will publish documentation to provide data subjects with sufficient awareness of the following, via a privacy notice or notices:

- what the organisation is and what it does, including contact details;
- contact details of the data protection officer (DPO);
- how personal data is used (the purpose);
- why personal data is used (the lawful basis);
- the categories of personal data used;

- the rights of individuals[4] with regard to the processing of their personal data, including the right to withdraw consent (if applicable);
- the recipients or categories of recipients of the personal data
- the details of transfers of the personal data to any third countries or international organisations (if applicable);
- the retention periods for the personal data;
- the rights available to individuals in respect of the processing;
- the right to lodge a complaint with the ICO;
- the source of the personal data (if the personal data is not obtained from the individual it relates to);
- the details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to);
- the details of the existence of automated decision-making, including profiling (if applicable)

6.7 This privacy information will be available as applicable:

- at the time personal data is collected from a data subject; or
- where personal data is obtained from another source
  - within a reasonable period of obtaining the personal data and no later than one month;
  - if RQIA intends to communicate with the individual, at the latest, when the first communication takes place; or
  - if RQIA intends to disclose the data to someone else, at the latest, when the data is disclosed

6.8 RQIA will ensure that this privacy information is provided in a way that is concise, transparent, intelligible, easily accessible and in clear and plan language

6.9 RQIA will regularly review and, where, necessary, update this privacy information. Where it is intended to use personal data for a new purpose, this privacy information will be updated and communicated accordingly, prior to any new processing commencing

7. Purpose Limitation

7.1 RQIA must only process personal data for specified, explicit and legitimate purposes, as set out in privacy information within Section 5.

7.2 Personal data may only be processed for new or different purposes from those disclosed when it was first obtained, if:

- the new purpose is compatible with the original purpose;
- specific consent is obtained for the new purpose; or
- RQIA can point to a clear legal provision requiring or allowing the new processing in the public interest.

7.3 Where this further processing is not based on the data subject's consent or on a lawful exemption from data-protection law requirements, the following should be used to assess whether a purpose is incompatible[5] with the original purpose:

[4] Refer to Appendix 1 for further details

[5] By way of example, provided that prescribed safeguards are implemented, further processing for scientific or historical research purposes or for statistical purposes will not be regarded as incompatible. Safeguards include ensuring data minimisation (e.g.

- the link between the original purpose/s for which the personal data was collected and the intended further processing;
- the context in which the personal data has been collected – i.e. whether the data subject would reasonably anticipate the further processing of their personal data;
- the nature of the personal data in particular whether it involves special categories of personal data (i.e. sensitive) or personal data relating to criminal offences/convictions;
- the consequences of the intended further processing for the data subjects;
- the existence of any appropriate safeguards e.g. encryption or pseudonymisation

7.4 In line with Section 5 of this policy, any changes in, or additions to, purpose must be made available to the data subject(s) prior to the processing commencing

- personal data Ensure the quality of personal data processed

8. Purpose Limitation

8.1 Personal data processed must be adequate to ensure that RQIA can fulfil the purpose(s) for which it was intended to be processed, and must have a rational link to that purpose(s).

8.2 Personal data should be limited to what is necessary, and not processed unless it is relevant for the purposes for the purposes intended

8.3 Staff must only process personal data as part of the discharge of their role within RQIA, and never for any reason unrelated to their job duties.

8.4 Personal data must be periodically reviewed to ensure it remains adequate, relevant and limited.

9. Accuracy

9.1 The accuracy of personal data must be checked at the point of collection, and at appropriate intervals thereafter.

9.2 All reasonable steps must be taken to amend inaccurate data as soon as possible after an inaccuracy is noticed.

9.3 Personal data must be held centrally, in the correct location, and in as few places as necessary. Staff should not create any unnecessary additional data sets.

9.4 Where applicable, RQIA must comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.

9.5 RQIA will keep a note of any challenges to the accuracy of the personal data

pseudonymisation or anonymisation where possible), the research will not be carried out for the purposes of making decisions about particular individuals and it must not be likely to cause substantial damage/distress to an individual, unless it is approved medical research

10. Storage Limitation

10.1 Personal data must not be kept in a form that allows data subjects to be identified for longer than needed for the purposes that it has been processed for.

10.2 Personal data must be regularly reviewed. Where personal data is no longer needed for specified purposes, all reasonable steps must be taken to delete it in accordance with regional retention schedule ('Good Management, Good Records' – GMGR') or to anonymise it. For further information on retention of information and records, please refer to BSO and RQIA's Records Management Policy.

10.3 RQIA must identify where personal data is required to be kept for public interest archiving, scientific or historical research, or statistical purposes.

10.4 RQIA must consider, and document, any requests for erasure under the 'right to be forgotten'.

11. Integrity and Confidentiality

11.1 RQIA is required to implement and maintain appropriate safeguards to protect personal data, taking into account in particular the risks to data subjects presented by unauthorised or unlawful processing or accidental loss, destruction of, or damage to their personal data.

11.2 Safeguarding will include:

- the use of encryption and pseudonymisation where appropriate;
- protecting the confidentiality (i.e. that only those who need to know and are authorised to use personal data have access to it), integrity and availability of the personal data

11.3 Staff must familiarise themselves with all the requirements as set out within the Information Security Policy, including:

- Clear desk and screen environments
- Appropriate use of email communications
- Use of removeable media
- Use of internet services
- Asset management
- Data Transfer
- Encryption
- Incident identification and reporting
- Remote and mobile working

11.4 Personal data must not be transferred outside of the United Kingdom unless:

- UK adequacy regulations are in place about the country or territory where the receiver is located or a sector which covers the receiver;
- Appropriate safeguards, as referred to within UK GDPR, are in place and a risk assessment conducted to the satisfaction that about the country or territory where the receiver is located or a sector which covers the receiver;
- An exception[6], as set out within Article 49 of the UK GDPR, applies

11.5 RQIA will ensure there are mechanisms in place to report breaches of the

[6] Please refer to ICO Guidance, available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/

processing of personal data7. Further information on reporting data breaches, including responsibilities for reporting, can be found within online guides[8]

11.6 RQIA's data protection officer on behalf of RQIA will be responsible for investigating and responding to any reported breaches, including correspondence with the ICO as appropriate.

12. Accountability

12.1 RQIA will ensure that, where required, contracts or other formal agreements are in place. Such contracts will include responsibility and liability

12.2 RQIA will document its processing activities. In line with Article 30 of UK GDPR, these will be (where applicable):

- the name and contact details of each data controller or data processor it engages with;
- the purpose of the data processing (where RQIA is deemed a data controller);
- a description of the categories of data subjects (where RQIA is deemed a data controller);
- a description of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations (where RQIA is deemed a data controller);
- transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- a general description of the technical and organisational security measures

12.3 In line with Article 35 of the UK GDPR[9], BSO on behalf of RQIA will conduct a 'Data Protection Impact Assessment' (DPIA)[10]. This will be completed if a project or the introduction of a new service, system, means of processing or policy is likely to result in a high risk to the privacy of individuals. Such high risk processing may include where RQIA intends to:

- evaluation or scoring;
- automated decision-making with legal or similar significant effect;
- systematic monitoring;
- sensitive data or data of a highly personal nature;
- data processed on a large scale;
- matching or combining datasets;
- data concerning vulnerable data subjects;
- innovative use or applying new technological or organisational solutions;
- preventing data subjects from exercising a right or using a service or contract

[7] All known or suspected breaches of personal data must be reported directly to RQIA's data protection officer, preferably via https://hrcs.hscni.net/data-breach-reporting/

[8] https://RQIA.sharepoint.hscni.net/sites/cs/IG/IG%20Guides

[9] Article 35 of the UK GDPR states that it is the data controller that is responsible for conducting the DPIA. Where RQIA is not considered the data controller, nevertheless this activity may be delegated to RQIA.

[10] A template is available at: https://RQIA.sharepoint.hscni.net/sites/cs/IG/IG%20Templates/20230126_DPIA_v3.0.docx?Web=1

12.4 The purpose of the DPIA is to ensure that privacy risks are mitigated including promptly addressing any identified issue while allowing the aims of the processing to be met whenever possible. Therefore, even if the processing is not considered high risk, a DPIA must nevertheless be completed in order to fully document the processing activity, as well as, as a minimum:

- the lawful basis;
- necessity and proportionality;
- data sharing arrangements;

12.5 BSO and RQIA have key staff in place to support the organisation's compliance with data protection legislation[11]. This includes:

- A Data Protection Officer (DPO);
- A Senior Information Risk Owner (SIRO);
- A Personal Data Guardian (PDG)

12.6 BSO and RQIA has a suite of training courses available to staff

13. Disclosure of data after a data subject's death

13.1 Data protection legislation does not apply to the data of those who are deceased.

13.2 Nevertheless, in line with published guidance[12], RQIA considers that there is an ethical obligation requiring that confidentiality obligations continue to apply after death.

13.3 RQIA will therefore consider the duty of confidentiality as set out by the Department of Health (DoH) code of practice[13] in the release of information pertaining to the deceased.

14. Monitoring

14.1 Each RQIA business unit / function will be expected to put in place the means by which performance against this policy can be assessed. This will consist of local policies, processes and procedures, as well as appropriate resources, responsibilities and accountabilities for data protection.

15. Non-Compliance

15.1 A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action.

In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law.

15.2 Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

[11] Specific roles are recorded in RQIA's Information Governance Assurance Framework
[12] https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality
[13] https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information

16. Review

16.1 This policy shall be reviewed regularly, and as a minimum:

- every 3 years; or
- following receipt of new information; or
- following updates to applicable legislation, guidance or best practice; or
- upon implementation of new agreements which may affect the policy

17. Equality Statement

17.1 This policy has been screened for equality implications as required by Section 75 of the Northern Ireland Act 1998 and it was found that there were no negative impacts on any grouping. This policy will therefore not be subject to an Equality Impact assessment.

Appendix 1 – Processing SARs

a) Rights of the Individual

The UK GDPR gives individuals specific rights over their personal data. For general data processing under the UK GDPR, in summary these are:

- the right to access personal data held about them (the right of subject access);
- the right to be informed about how and why their data is used - and you must give them privacy information;
- the rights to have their data rectified, erased or restricted in limited circumstanced;
- the right to object in limited circumstances;
- the right to portability of their data in limited circumstances; and
- the right not to be subject to a decision based solely on automated processing.

Further information on these rights, including where they may not apply, are set out within ICO guidance[14].

b) Defining a valid request:

In line with ICO guidance[15], an individual may submit a request to exercise their rights verbally or in writing. The term 'in writing' covers requests submitted by letter and electronic form, including those sent via Social Media. The request does not have to make any direct reference to the UK GDPR or DPA 2018, or reference the term 'Subject Access Request', or be the sole or main theme of the requester's correspondence.

All requests from a data subject to exercise their rights must be processed via the BSO's Data Protection Officer on behalf of RQIA, or delegate, and as such must be sent onwards immediately.

RQIA defines a request 'received' when it is delivered to BSO or RQIA (for example, to the inbox of a member of staff), and not the date the request is forwarded for onward processing[16]. Any SARs must therefore be forwarded to BSO's Information Governance team[17] immediately for onward processing.

c) 'Business As Usual' Requests

It is important to draw a practical distinction between formal requests for information and routine verbal enquiries and correspondence that you can deal with in the normal course of business. Where information can be provided routinely and you can respond quickly, BSO on behalf of RQIA should endeavour to process the request in 'the normal course of business' rather than as a formal SAR. However, the SAR process may be appropriate where an individual requests a high volume of information and you need to conduct a time-consuming search of records in order to comply with the request.

If staff are in doubt as to whether a request is to be processed via normal course of business or via formal SAR, they should contact RQIA's Information Governance office to discuss in the first instance.

---

[14] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/the-rights-of-individuals/

[15] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

[16] In respect of emails, however, where an automated 'out of office' message provides instructions on how to re-direct a message, the request would not be 'received' until it was re-sent to the alternative contact.

[17] dpa.RQIA@hscni.net

The BSO DPO on behalf of RQIA, has the authority to direct requests that should be actioned as a standard response to general enquiries.

d) Identity of the applicant and reasons for the request

In keeping with ICO advice[18], BSO on behalf of RQIA must be satisfied of the identity of the requestor, and that the data held relates to the individual in question. Therefore, when required, reasonable and proportionate identity checks should be sought.

e) Requests from third parties

An individual may ask a third party (e.g. a relative, friend or solicitor) to make a request on their behalf. Before responding, BSO on behalf of RQIA needs to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

f) Time Limits for Compliance with Requests

BSO on behalf of RQIA must comply with a request without undue delay and at the latest within one month of receiving the request. BSO on behalf of RQIA can extend the time to respond by a further two months if the request is complex or if BSO on behalf of RQIA has received a number of requests from the individual, e.g. other types of requests relating to individuals' rights.

If RQIA processes a large amount of information about an individual, it may be able to ask them to specify the information or processing activities their request relates to, if it is not clear. The time limit for responding to the request is paused until clarification is provided, although BSO on behalf of RQIA should supply any of the supplementary information possible within one month."

If it becomes clear at any stage that the above timescales cannot be met (i.e. the statutory deadline or extended deadline), BSO on behalf of RQIA will inform the applicant in writing, in advance of this deadline, and give a revised deadline for completion.

g) Means by which information will be conveyed

In line with ICO guidance[19], responses and any information held will be provided in a commonly used format of BSO's choosing on behalf of RQIA, unless the requestor makes a reasonable request for it to be provided in another commonly used format.

h) Refusing a request

In certain circumstances, BSO on behalf of RQIA and / or RQIA may not be obliged either to comply with a request from a data subject to exercise their rights.

The right to be forgotten will not apply where processing is necessary:

- for exercising the right of freedom of expression and information;

[18] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-should-we-consider-when-responding-to-a-request/#ID

[19] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/how-should-we-supply-information-to-the-requester/#format

- for compliance with a legal obligation which requires processing under domestic law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

The right to restriction of processing will only apply where one or more of the following is relevant:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
  the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
  the data subject has objected to processing pursuant to Article 21(1) of UK GDPR ('right to object') pending the verification whether the legitimate grounds of the controller override those of the data subject.

The right to object will only apply where BSO on behalf of RQIA is relying on 'public task' or 'legitimate interests' as a lawful basis to process personal data.

The right to portability will only apply where BSO on behalf of RQIA is relying on consent or the 'performance of a contract' as the lawful basis to process personal data.

Exemptions[20] from the obligation to respond to a SAR include:

- Crime and taxation: general
- Crime and taxation: risk assessment
- Legal professional privilege
- Functions designed to protect the public
- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Judicial appointments, independence and proceedings
- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest
- Health, education and social work data
- Child abuse data
- Management information
- Negotiations with the requester
- Confidential references
- Exam scripts and exam marks

[20] Where an exemption applies, RQIA may refuse to provide all or some of the requested information, depending on the circumstances.

In addition, BSO on behalf of RQIA will take into account appropriate guidance from the ICO[21] in determining whether it believes a request is manifestly unfounded or excessive.

In all circumstances where an exemption applies, BSO on behalf of RQIA will inform the individual of:

- the individual of:
- the reasons why[22];
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through the courts.

BSO on behalf of RQIA may also refuse a SAR if it deems it manifestly unfounded or excessive. In such circumstances, BSO on behalf of RQIA must be able to demonstrate this to the individual.

i) Charging a fee

RQIA will not normally charge a fee. However, if a request is deemed manifestly unfounded or excessive, because of their repetitive character or when the request relates to large amounts of data , BSO on behalf of RQIA may charge a 'reasonable fee' to cover administrative costs.

j) Complaints

BSO on behalf of RQIA will advise, via a privacy notice, of a data subject's right to complain to the ICO.

BSO on behalf of RQIA will advise all data subject, who have submitted a SAR, of their right to seek an internal review of its handling of a request. In such circumstances, a review panel will be convened, in line with Section 12 of BSO's Freedom of Information and Environmental Information Policy.

Internal review panels will consist of two RQIA members of staff with no involvement in the original handling of the request, and preferably:

- An Executive Director
- A Non-Executive Director

The panel will be facilitated by the IG team and/or Head of Corporate Services

The panel will consider decisions made, rationale, timeliness and whether all appropriate personal data has been provided.

BSO on behalf of RQIA will conduct internal reviews and relay the outcome to the applicant within one calendar month of receipt of a request for review

Applicants will be advised that they may exercise their right to appeal to the ICO should they remain dissatisfied with the outcome of the internal review.

[21] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/when-can-we-refuse-to-comply-with-a-request/#refuse1

[22] Where an exemption applies, the reasons you give to an individual for not complying with a request may depend upon the particular case. For example, if telling an individual that you have applied a particular exemption would prejudice the purpose of that exemption, your response may be more general. However, where possible, you should be transparent about your reasons for withholding information.

k) Transferring Requests for Information

RQIA and BSO on RQIA's behalf will not contact another public authority on the applicants' behalf to transfer the request. However, in circumstances where BSO on RQIA's behalf believe that the information requested is held by another public authority, it will:

- advise the applicant that BSO/RQIA will not be taking the request further;
- provide contact details of that authority, where possible

Review and Monitoring

This framework will be reviewed every three years by IGG to ensure compliance with legislation and the requirements of the IMAC. Recommendations for amendment will be reported to the SIRO.

Equality Statement

This policy has been screened for equality implications as required by Section 75 of the Northern Ireland Act 1998 and it was found that there were no negative impacts on any grouping. This policy will therefore not be subject to an Equality Impact assessment.

Freedom of Information and Environmental Information Policy

Title:	Freedom of Information and Environmental Information Policy		
Ownership:	Information Governance Group		
Approved by:	Policy Group EMT BARC Authority	Date Approved	9 October 2025 14 October 2025 6 November 2025 11 December 2025
Date Implemented:		Date for Review	01.04.2028
Version No.	2.1	Supersedes:	V 2.0
Key Words:	Freedom of Information, Environmental Information		
Director Responsible:	Chair of Information Governance Group		
Links to other Policies, Procedures & Guidance	Information Governance Policy		
	Information Security Policy		
	Records Management Policy		
	Data Protection & Confidentiality Policy		

Contents

1. Introduction

1.1 The Freedom of Information Act 2000 (FOI) gives the public a general right of access to information held by a public authority, subject to certain conditions and exemptions. FOI promotes greater openness and accountability across the public sector, therefore facilitating a better understanding of how public bodies carry out their business and how they spend public money.

1.2 FOI places a statutory obligation on the Business Services Organisation (BSO and RQIA) to publish details of all recorded information that it holds where requested, except where an exemption or other ground for refusal of a request under the FOI Act applies. FOI is wholly retrospective and applies to all recorded information held by public authorities regardless of its date.

1.3 The Environmental Information Regulations 2004 (EIR) gives the right to access 'environmental information' held by public authorities, and therefore requires similar measures for all environmental information held by RQIA.

2. Purpose

2.1 RQIA acknowledges its obligations as set out under FOI and EIR, and is committed to the principles of openness, transparency and accountability.

2.2 This policy establishes a framework which underlines the commitment. The purpose of this policy and related procedures is to ensure that RQIA is compliant with the FOI and EIR, and sets out the procedures for dealing with requests for information.

3. Supporting Legislation

3.1 This policy has been written to support staff in compliance with the following legislation and policy requirements and best practice guidance, as set out within The Business Services Organisation's (BSO and RQIA's) Information Governance Assurance Framework

4. Scope

4.1 The scope of this policy is to support compliance against FOI and EIR. The policy will cover all recorded information held by RQIA otherwise than on behalf of another person, or held by another person on behalf of RQIA and is concerned with all information systems, electronic and non-electronic information. It applies to all directorates, services and departments, and all staff.

4.2 Information is considered 'held' in any format (hard copy, or electronic) if it is retained by RQIA for the purposes of its business.

4.3 Under FOI and EIR, RQIA is required to provide any information it holds, unless it can demonstrate that an exemption or exception, respectively,

applies.

4.4 This policy covers all forms of recorded information held, including personal data as defined in data protection legislation, as well as organisational, business and operational information.

5. Roles and Responsibilities

5.1 Roles and Responsibilities are as set out within RQIA's and BSO's Information Governance Assurance Framework, which is available on request.

6. Defining a valid request

6.1 As defined in Section 8 of the FOI Act, to meet all the requirements of a valid FOI request, a request must:

- Be in writing[1]
- State the name of the applicant and a valid address[2] for correspondence
- Describe the information requested
- Be received in a legible form

6.2 The EIR does not specify how a valid request must be made. Requests for information under EIR can therefore be made in writing or verbally. However, as the EIR states that responses should be in writing, BSO on behalf of RQIA will also need to ask the applicant for a name and contact details for correspondence.

6.3 A request is deemed as 'received'3 when it is delivered to BSO on behalf of or to RQIA directly (for example, to the inbox of a member of staff or in the case of a request made under EIR, also at the point in which a verbal request is received), and not the date the request is forwarded for onward processing[4].

6.4 Any requests for information under FOI or EIR must therefore be forwarded to RQIA's Information Governance team[5] immediately for onward processing.

7. Identity of the applicant and reasons for the request

7.1 The ICO has advised that, as FOI enables disclosure on grounds of public interest, responses should be applicant and motive blind. BSO on behalf of RQIA will therefore assess all requests on the understanding that applicant identity is not a relevant consideration. Possible exceptions to this include:

- to be satisfied that an FOI request is valid under Section 8 of FOI

---

[1] The term 'in writing' covers requests submitted by letter and electronic form, including those sent via Social Media.

[2] In line with ICO guidance, a valid address is any address where the requester may be contacted (including postal or email addresses) and does not have to be their normal residential or business address

3 Where BSO has sought clarification in order to identify and locate the requested information, the request will only be deemed as 'received' only once this sufficient clarification is provided. In line with ICO guidance, this clarified request will represent a new request for information.

[4] In respect of emails, however, where an automated 'out of office' message provides instructions on how to re-direct a message, the request would not be 'received' until it was re-sent to the alternative contact[6] The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

[6] The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

- to consider whether a request is deemed to be repeated (FOI only);
- to consider if a request, or requests, are vexatious and/or manifestly unreasonable;
- to consider whether disclosure would be contrary to Data Protection principles or would be likely to endanger the health and safety of any person;
- to consider aggregated costs in line with Fees Regulations[6] (FOI only);
- to determine whether the information is accessible by other means

8. Time Limits for Compliance with Requests

8.1 BSO on behalf of RQIA aims to respond to FOI and EIR promptly, and as soon as possible within the 20 working day limit.

8.2 In line with Section 10 of FOI, and the Freedom of Information Code of Practice, BSO on behalf of RQIA may exceed the 20 working day limit if information falls within the scope of a qualified exemption and additional time is required to consider the public interest test. Where this is the case, BSO on behalf of RQIA will inform the applicant to advise of which exemption(s) it is currently considering. BSO on behalf of RQIA will also inform the applicant of a revised deadline, which should exceed an additional 20 working days. If the deadline has to be further extended, BSO on behalf of RQIA will write further to the applicant to advise.

8.3 If it becomes clear at any stage that RQIA cannot meet the statutory obligations, BSO on behalf of RQIA will inform the applicant of this, alongside an apology, and advise that it will provide a response as soon as possible.

9. Means by which information will be conveyed

9.1 When an applicant expresses a preference for communication by particular means, BSO on behalf of RQIA so far as is reasonably practicable, will give effect to that preference.

9.2 In determining what is reasonably practicable, BSO on behalf of RQIA will consider all the circumstances, including the cost of doing so. If it is determined that it is not reasonably practicable to comply with any preference expressed by the applicant, the applicant will be notified of the reasons for its determination and will provide the information by such means as which is deemed reasonable.

10. Approval and Signature

10.1 In line with BSO and RQIA procedures, all responses to requests made under FOI and EIR will be approved by the relevant director and CEO before release. Please refer to the BSO Corporate Services 'Information Requests Standard Operating Procedure' for further details on this.

[6] The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

11. Refusing requests

11.1 Part II of FOI[7] and Part 3 of EIR set out a number of exemptions and exceptions (respectively), whereby BSO on behalf of RQIA may refuse to supply information. There are two categories of exemption:

- absolute exemptions: where there is no obligation under the FOI to release the requested information
- qualified exemptions/exceptions: where BSO on behalf of RQIA must assess the balance of the public interest for and against disclosure. The arguments against need to outweigh those in favour to justify non-disclosure. This is known as a 'public interest test'. All exceptions in the EIR are qualified.

11.2 In considering any exemption and public interest test, BSO on behalf of RQIA may[8] consult with appropriate third parties, when:

- requests for information relate to persons or bodies who are not the applicant and/or RQIA; or
- disclosure of information is likely to affect the interests of persons or bodies who are not the applicant or RQIA

11.3 Where BSO on behalf of RQIA is specifically considering the applicant of Section 36 of FOI ('Prejudice to effective conduct of public affairs'), the opinion of the Qualified Person[9] will be sought prior to a response being issued to the applicant.

11.4 While the view of any third party will assist in the assessment of any exemptions, RQIA will make any final determination on release or withholding of information it holds.

11.5 Where an exemption or exception is applied, BSO on behalf of RQIA will advise the applicant of this, unless (and where applicable) doing so would involve the disclosure of any information which falls within the scope of an exemption of exception. In such circumstances, BSO on behalf of RQIA will neither confirm nor deny that it holds information.

11.6 Section 12 of FOI gives BSO and RQIA provision to refuse to provide information where it estimates that it would exceed the appropriate limit. The appropriate limit is established under the Fees Regulations (see footnote 6) as £450, or 18 hours work as per ICO guidance[10]. The appropriate limit should be considered before any exemptions in Part 2 of FOI.

11.7 No 'appropriate limit' is set by EIR. However, BSO on behalf of RQIA reserves

[7] Further information on the FOI exemptions can be found via the National Archives
[8] BSO may consider that consultation is not appropriate where the cost of consulting with the third party would be disproportionate or the view of the third party can have no effect on the decision as to whether to disclose
[9] As set out within Section 36(5) of FOI
[10] https://ico.org.uk/media/for-organisations/documents/1199/costs_of_compliance_exceeds_appropriate_limit.pdf

the right to refuse to comply with requests under Section 12(4) of EIR which are 'too general'.

11.8 BSO on behalf of RQIA can only include certain tasks when estimating whether responding to a request will exceed the appropriate limit. These are:

- establishing whether information is held;
- locating and retrieving the information; and
- extracting the relevant information from a document containing it

11.9 If BSO on behalf of RQIA is using the cost limit as grounds for refusing the request, the following will also apply. BSO on behalf of RQIA will:

- provide a written refusal notice, stating that complying with the request would exceed the appropriate cost limit;
- issue a fees notice advising the applicant of the amount to be charged in for complying with the request;
- state whether the information is held, unless finding this out would in itself incur costs over the limit;
- provide the applicant with reasonable advice to refine (change or narrow) their request, including explaining why the limit would be exceeded and what information, if any, may be available within the limits.

11.10 If the requester refines their request appropriately, BSO on behalf of RQIA will then deal with this as a new request in line with Section 6.4 of this policy.

11.11 Section 14 of FOI gives BSO and RQIA provision to refuse a request where it is considered vexatious or repeated. Regulation 12(4) of the EIR gives BSO and RQIA provision to refuse a request that is considered to be manifestly unreasonable.

11.12 In determining whether a request is vexatious or manifestly unreasonable, and in line with ICO guidance[11], BSO on behalf of RQIA will consider all the circumstance including, but not limited to:

- the burden (on the public authority and its staff);
- the motive (of the requester);
- the value or serious purpose (of the request); and
- any harassment or distress (of and to staff).

11.13 BSO on behalf of RQIA will consider a request to be repeated when all three of the following criteria have been fulfilled:

- the request is identical or substantially similar to a previous request from the same applicant;
- RQIA has previously provided the information to the applicant or confirmed that information is not held in response to an earlier FOIA request; and
- a reasonable interval[12] has not elapsed between the new request and your compliance with the previous request.

[11] https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-information-regulations/dealing-with-vexatious-requests-section-14/

[12] While this is not defined, ICO guidance states that this should consider:

- the likelihood that the information will differ significantly from what has been previously provided; and

11.14 Where a request is considered repeated, BSO on behalf of RQIA will provide the applicant with a refusal notice.

11.15 In addition, RQIA will not be obliged to respond to a request made under provision of FOI or EIR, if this would mean creating new information or providing an opinion or judgement that is not already recorded.

12. Internal Review

12.1 In line with Section 17 of FOI and The Cabinet Office Freedom of Information Code of Practice ('The Code'), BSO on behalf of RQIA will advise all applicants within a response of their right to seek an internal review of its handling of a request.

12.2 In line with Paragraph 5.3 of The Code, RQIA will not be obliged to accept a request for internal review not made within 40 working days from the date the initial response to the applicant was issued. RQIA will make this clear in its initial response

12.3 BSO on behalf of RQIA will only accept requests for internal review that are made in writing.

12.4 Internal review panels will consist of at least two RQIA members of staff, one RQIA member of staff with no involvement in the original handling of the request, and preferably chaired by the RQIA Chairperson, with other senior staff as appropriate.

12.5 The panel will be facilitated by the BSO IG team and/or Head of Corporate Services

12.6 The panel should make a fresh decision based on all the available evidence that was relevant at the date of the request for information. This should include

- how the request was handled and the initial response, including reserving the right to interview members of staff involved in the original decision;
- whether the relevant information was identified;
- whether it wishes to uphold the original exemption(s) (if applicable), or apply a different or different exemption(s) if applicable

12.7 BSO on behalf of RQIA will conduct internal reviews and relay the outcome to the applicant within 20 working days of receipt of such a request, or 40 working days in exceptional circumstances.

12.8 Applicants will be advised that they may exercise their right to appeal to the ICO should they remain dissatisfied with the outcome of the internal review.

- the amount of time that has passed (if it is unlikely that the information will differ in any significant way) since BSO complied with the previous request

13. Transferring Requests for Information

13.1 BSO and RQIA will not contact another public authority on the applicants' behalf to transfer the request. However, in circumstances where RQIA believe that the information requested is held by another public authority, it will:

- advise the applicant that RQIA will not be taking the request further;
- provide contact details of that authority, where possible

13.2 In addition, RQIA will not accept requests transferred from another public authority to RQIA.

14. Publication Scheme

14.1 BSO and RQIA will maintain an 'approved model' Publication Scheme introduced by the ICO[13].

14.2 BSO on behalf of RQIA will maintain an online disclosure log[14] that lists responses to requests made to RQIA under FOI and EIR.

15. Non-Compliance

15.1 A failure to adhere to the policy and its associated procedures/guidelines mayresult in disciplinary action.

In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in breach of the law.

15.2 Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

16. Review

16.1 This policy shall be reviewed regularly, and as a minimum:

- every 3 years; or
- following receipt of new information; or
- following updates to applicable legislation, guidance or best practice; or
- upon implementation of new agreements which may affect the policy

16.2 BSO and RQIA's performance regarding this policy will be reviewed against compliance against legislation, policy and best practice, via Internal Audit.

17. Equality Statement

17.1 This policy has been screened for equality implications as required by Section 75 of the Northern Ireland Act 1998 and it was found that there were no

[13] http://www.hscbusiness.hscni.net/information/1707.htm
[14] http://www.hscbusiness.hscni.net/information/2971.htm

negative impacts on any grouping. This policy will therefore not be subject to an Equality Impact assessment.

Records Management Policy

RQIA

Title:	Records Management Policy		
Ownership:	Information Governance Group		
Approved by:	Policy Group EMT BARC Authority	Date Approved	9 October 2025 14 October 2025 6 November 2025 11 December 2025
Date Implemented		Date for Review	01-04-2028
Version No.	2.2	Supersedes:	v.2.0
Director Responsible:	Chair of Information Governance Group		
Key Words:	Records; records management; information; governance; record keeping; storage; retention; archiving; appraisal; tracking; destruction		
Links to other Policies, Procedures & Guidance	Information Governance Policy		
	Freedom of Information and Environmental Information Policy		
	Data Protection & Confidentiality Policy		
	Information Security Policy		

Contents

1. Introduction & Policy Statement

1.1 All Health and Social Care (HSC) records are public records under the terms of the Public Records Act (Northern Ireland) 1923 and in the Disposal of Documents (Northern Ireland) Order (1925). The RQIA (RQIA) therefore has a statutory duty to make arrangements for the safe keeping and eventual disposal of its records.

1.2 Further, information is a corporate asset and the records of the RQIA are important sources of service user and client information in addition to administrative, financial, legal, evidential and historical information. They are vital to the organisation in its current and future work, for the purposes of accountability, and for an awareness and understanding of its history. They are the corporate memory of the organisation.

1.3 Records Management is the process by which RQIA will manage all the aspects of its records, from their creation, all the way through to their lifecycle to their eventual disposal or permanent preservation (known as the 'records lifecycle').

1.4 Good records management is therefore critical in the discharge of RQIA's services, and in order to evidence its strategic objectives, as set out within its annual quality reports.

1.5 RQIA is therefore committed to the creation, maintenance and management of its records, and to document its principal activities.

1.6 It is therefore essential that all records are managed effectively within a robust framework, in accordance with best practice and legislative and policy requirements, as set out within RQIA's & BSO Information Governance Assurance Framework

2. Purpose and Aims

2.1 The purpose of this policy is to ensure that RQIA adopts best practices in the management of its records so that authentic, reliable and useable records are created, maintained and managed, which are capable of supporting business functions and activities for as long as they are required, and which assist to support and evidence its strategic objectives, as set out within its annual quality reports

2.2 Compliance with this policy will help RQIA ensure that:

- records are made accessible to enable well-informed and proper judgments to be made;
- records are kept securely and protected from accidental loss, destruction and unauthorised access;
- records are kept for no longer than is necessary, in accordance with legal and professional obligations and with due regard to the regional retention and disposal schedule, known as 'Good Management, Good Records' (GMGR);
- staff are made aware of the requirements on them in the management of records within their sphere of work or responsibility

2.3 Compliance with this policy will also help evidence RQIA's accountability, through management of information about its decisions and activities.

3. Scope

3.1 The international standard of managing records, ISO 15489 defines a record as *"information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business"*.

3.2 ISO 15489 also describes the characteristics of 'Authoritative Records' as being authentic, reliable integral and useable.

3.3 In the context of this policy a record is therefore any recorded information that contains information, in any media which is created, collected, processed, used, stored and/or disposed of by RQIA staff, as well as those acting as its agents in the course of RQIA business.

3.4 This policy is designed to assist RQIA with the controlled method in which information and records should be managed throughout their lifecycle. Requirements for this are set out within subsequent sections of this policy.

3.5 This policy applies to all directorates, services and departments, all staff, and as appropriate to contractors and third party service providers acting on behalf of RQIA.

4. Roles and Responsibilities

4.1 Responsibilities are as set out within RQIA's & BSO's Information Governance Assurance Framework, which is available on request.

5. Record Creation and Maintenance

5.1 Records should be organised into, and stored within, a file system or classification scheme upon creation, in order that they remain secure and appropriately accessible from the outset. This system or classification must include the business function that it pertains to.

5.2 Records will be named with meaningful titles, to allow for appropriate staff to identify them and any applicable record collections.

5.3 Records, or entries within them, must be factual, consistent, accurate, legible and easily understood.

5.4 Any alterations or additions to records must be made in such a way that the original can still be read.

5.5 All records must be appropriately accessible, so as to be used in a way consistent with the purpose for which it was created.

5.6 Records must be maintained for as long as the record is needed, despite any changes of formats (including software) and/or business processes/practices. Records will be protected during their life cycle by ensuring safe and adequate storage facilities or media.

5.7 Local procedures should be established for the titling, classification and indexing of records, according to the needs of the business unit or function.

5.8 All record-keeping system should be referenced within RQIA's Information Asset Register

5.9 Records, especially those containing personal data, should be regularly reviewed to ensure that they are accurate, relevant and limited. Where applicable, such records should be 'weeded' periodically to reduce the risks of inaccuracies and excessive retention.

6. Confidentiality and Access

6.1 All RQIA's records are public records, and therefore are subject to a number of statutory provisions regarding confidentiality, access and disclosure.

6.2 Specific guidance on matters of data protection and confidentiality, including access to personal data held within records, can be found within RQIA's Data Protection and Confidentiality Policy.

6.3 The Freedom of Information Act (2000) and Environmental Information Regulations (2004) provide members of the public with a general right of access to recorded information held by public authorities, which will include RQIA. The RQIA's Freedom of Information Policy covers this aspect of records management

7. Version Control

7.1 Version control is the management of multiple revisions to the same record. It is used to track the changes that occur to a record throughout its initial development and subsequent revision(s).

7.2 Version control is particularly important for electronic documents because they can easily be changed by a number of different users. Knowing the `appropriate' version of a document is vital to ensure compliance with current

7.3 In key documents subject to a period of development it is useful to display at the front of the document, a version control table showing the development history of the document and the version changes that have been applied.

7.4 The version control system adopted by RQIA uses numbers greater than zero with decimal points. Minor amendments equate to an incremental change to the number at the right of the decimal point, while a major[1] change will result in an incremental change to the number at the left. The following should be used as a guide:

- All new, draft documents should initially be numbered Version 0.1;
- Changes to this document would result in version 0.2, 0.3 (etc.) until the document is approved and becomes the 'final' version;
- When the document is approved for the first time, the number converts to Version 1.0 and the document is published
- Once published the number to the right will increase with each minor amendment approved (Version 1.1, 1.2 etc.)
- A major amendment to the document will result in the number to the left of the decimal point increasing by 1 and the number to the right returning to

zero (i.e. Version 2.0)

- In addition to adding the version number to the end of the file title, it should also be displayed within the document. The version number should appear on any document title page, and also in the header or footer of each page.

8. Record Storage, Movement and Tracking

8.1 When not in use, records (regardless of format) should be kept in a secure storage area. Records should be stored within the business unit that they are being used for, until such times as they are transferred (either to storage or for permanent preservation) or destroyed.

8.2 Physical records should be stored in an appropriate environment to ensure they remain fit for purpose until disposed of or transferred for permanent preservation. The following should be considered:

- Environment: Is the location suitable for the type of material being stored? Is the area free from hazards that may cause the records to deteriorate or place at risk staff that may need to access the records?
- Security: Is the level of security offered by the location acceptable for the type of record being stored?
- Ease of Access: Can records be easily located and retrieved?
- Layout: Consideration should be given to the design of the storage location to ensure the most cost-effective use is made of space available.

8.3 The movement and location of physical (i.e. non-electronic) records should be controlled to ensure that a record can be retrieved as required, and that there is a record of transactions associated with it,

8.4 Records that are no longer in current use can be transferred to secondary or archive storage more remote from the operational area.

8.5 When making arrangements to permanently move records external to RQIA premises (e.g. offsite storage or archive), consideration must be given to the security and confidentiality of the record in transit. Please refer to RQIA's Data Protection and Confidentiality Policy and Information Security Policy for further detail.

8.6 A comprehensive record should be maintained of any records sent for such storage including a proposed date for review/destruction.

8.7 Electronic records should be stored in such a way that throughout their lifecycle it can be recovered in an accessible format. Over time such changes as migration to new formats can cause documents to fail to open, impacting the integrity of the record. Any changes to electronic storage systems or structure used to hold records should only take place after full consideration of the impact on the records held and, ideally, successful testing of retrieval of transferred records from the new version/system.

9. Record Closure

9.1 A record should be closed when the business use for that record ceases.

9.2 Manual records should be clearly marked with the date of closure and planned review/disposal date. Closed records in electronic storage systems

should hold this information as part of the record's metadata and/or the record moved to another electronic area reserved for closed records.

10. Record Review / Appraisal

10.1 When the minimum retention period for a record or set of records, as set out within GMGR, has passed it should be subject to an appraisal. The purpose of the appraisal process is to:

- identify records to be considered for permanent preservation by The Public Record Office of Northern Ireland (PRONI)
- identify records to be retained for a longer period
- to confirm that records not meeting above criteria should be destroyed

11. Permanent Preservation

11.1 Certain records, as set out within GMGR, will meet the criteria for consideration of permanent preservation. This information is typically that which will enable the public to understand the working of the RQIA, the impact on the population it serves and which will likely have long term research value.

11.2 PRONI has responsibility for assessing the value of records for historical/research purposes and deciding whether or not they should be permanently preserved.

11.3 For such records, PRONI should be engaged, who will provide guidance and assistance as to next steps.

12. Retention Beyond Minimal Retention Period

12.1 GMGR sets out recommended minimum periods for retention of records. When a record is appraised, the following questions may assist in determining whether it should be retained beyond this minimum retention period:

- is there a continuing need to retain this record for the conduct of day-to-day business?
- is there clear evidence of a future need for constant reference to this record?
- will it be needed to deal with enquiries in the future?
- is the information needed for statistical analysis within the organisation?
- are there bodies of statistical information upon which future policies and forecasts may be based?
- is the information required for conducting legal proceedings in the event of a legal action being taken by, or against the organisation?
- is there a legal requirement to retain these records (e.g. Health and Safety regulations)?
- is there a financial need to retain these records (e.g. for audit purposes)?
- is there a professional reason (e.g. continuity of care, research, audit)?

12.2 Where it is determined that a record should be retained beyond this minimum retention period, the reasons should be clearly documented, and a data set to re-appraise the record. This should be no later than an additional 5 years.

13. Records Disposal

13.1 Following appraisal, any records not selected for permanent preservation or a longer retention period should be disposed of. However, no information should be destroyed if it is the subject of a current request under relevant legislation, or any other legal process, such as an inquest or public inquiry.

13.2 Paper records should be destroyed securely through a local process of industry-standard cross cut shredding, or availing of the BSO's & RQIA's confidential waste disposal service

13.3 Digital records should be destroyed either via overwriting the media a sufficient number of times, or the physical destruction of the media. Further advice about the destruction of digital records should be sought from RQIA's Information Technology Service (RQIA)

13.4 A record of destruction should be maintained.

14. Specific Record Types: Email

14.1 Personal email accounts tend to be structured according to personal preference. The data held within an email account is not routinely searchable or organised in a systematic way, making email accounts unsuitable for record storage purposes.

14.2 Email accounts should therefore not be used to file records on a permanent basis, but should be regarded as transient storage areas for working documents.

14.3 E-mails or documents distributed by e-mail that need to be retained as RQIA records should be moved to the appropriate paper or electronic system and the e-mail copy destroyed as soon as practicable.

14.4 Where email is declared as a record or as a component of a record, the entire email must be retained, including attachments, so the record remains integral - for example an email approving a business case must be saved with the business case file.

15. Specific Record Types: Scanned Records

15.1 Where paper records are scanned, the main consideration is that the information can perform the same function as the paper counterpart did, and like any evidence, scanned records can be challenged in a court.

15.2 Providing scanning is carried out to an acceptable standard, and quality assured, original documents should be destroyed after scanning, in order to prevent duplication.

16. Non-Compliance

16.1 A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action.

In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution and open to claims for damages if their actions are found to be in

breach of the law.

16.2 Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

17. Monitoring

17.1 Each RQIA business unit / function will be expected to put in place the means by which performance against this policy can be assessed. This will consist of local policies, processes and procedures, as well as appropriate resources, responsibilities and accountabilities for record keeping and the maintenance of activities.

18. Review

18.1 This policy shall be reviewed regularly, and as a minimum:

- every 3 years; or
- following receipt of new information; or
- following updates to applicable legislation, guidance or best practice; or
- upon implementation of new agreements which may affect the policy

19. Equality Statement

19.1 This policy has been screened for equality implications as required by Section 75 of the Northern Ireland Act 1998 and it was found that there were no negative impacts on any grouping. This policy will therefore not be subject to an Equality Impact assessment.