Business Services Organisation

Information Governance Policy

Produced by the Human Resources and Corporate Services Directorate
Business Services Organisation
2 Franklin Street, Belfast, BT2 8DQ

Reference No:

Title:	Information Governance Policy		
Author(s):	Alan McCracken		
Ownership:	Director of Human Resources and Corporate Services		
Approval By:	BSO Board	Approval Date:	24/05/2018
Operational Date:	24/05/2018	Next Review:	24/05/2020
Version No.	3.0	Supersedes:	2.0
Key Words:	Information Governance, Data Protection, Information Security, Freedom of Information		
Director Responsible:	Director of Human Resources and Corporate Services		
Lead Author:	Alan McCracken		
Lead Author Position:	Data Protection Officer		
Additional Author(S):			
Department:	Corporate Services		
Contact Details:	dpa.bso@hscni.net		
Links to other Policies:	Information Security Policy		
	Data Protection & Confidentiality Policy		
	Freedom of Information Policy		
	Records Management 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 BSO represents one of their most valuable assets, and core to most of the services delivered to their service users, business partners and customers. It is therefore essential that all information is managed effectively within a robust framework, in accordance with best practice and the legislative framework which includes:

- General Data Protection Regulation (GDPR) 2016
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order 1925
- Re-Use of Public Sector Information Regulation 2005
- Access to Health Records (Northern Ireland) 1993
- Human Rights Act 1998
- Audit & Internal Control Act 1987
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Health and Social Care (Reform) Act 2009
- Public Interest Disclosure Act 1998
- The Investigatory Powers Act 2016
- Guidance from the Information Commissioners Office
- The Department of Health (DoH) Good Management, Good Records(GMGR)
- DoH Information Management Assurance Checklist (IMAC)

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 Business Services Organisation (BSO) 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 need to share identifiable personal information 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 BSO and its employees 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 the BSO should be open for public scrutiny, it is acknowledged that some information, which is commercially sensitive, may need to be safeguarded.

2 Purpose

The IG requirements set out within this policy and subsequent 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

2.1 This policy 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 information governance.

2.2 The IG requirements set out within this policy and subsequent 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, personal information 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 assets. The policy will cover all information within the BSO and is concerned with all information systems, electronic and non-electronic. It applies to all directorates, services and departments, all permanent and temporary staff, all agency workers, and as appropriate to contractors and third party service providers acting on behalf of the organisation.

3.2 IG covers all information held, and all information systems used to hold that information. This includes, but is not necessarily limited to:

- stored on computers
- transmitted across internal and public networks such as email or Intranet/Internet
- stored within databases
- printed or handwritten on paper, whiteboards (etc.)
- sent by facsimile (fax), telex or other communications method

- stored on removable media such as CDs, hard disks, pen drives, tapes and other similar media
- stored on fixed media such as hard drives and disk subsystems
- held on film or microfiche
- paper and electronic structured records systems
- information recording and processing systems whether paper electronic video or audio records
- presented on slides, overhead projectors, using visual and audio media
- spoken during telephone calls and meetings or conveyed by any other method.

3.3 This policy covers all forms of information held, including (but not limited to):

- Information about members of the public
- Non- employees on organisational premises
- Staff and personal information
- Organisational, business and operational information.

3.4 This policy covers all information systems purchased, developed and managed by/or on behalf of, the BSO and any individual directly employed or otherwise used by the BSO.

4 Policy

There are seven key, interlinked strands to this policy

- Openness.
- Legal compliance.
- Information security.
- Quality assurance.
- Information risk management.
- Records management
- Training and awareness.

4.1 Openness

This policy recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Confidential information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the requirements outlined in Data Protection Legislation[1]

Non-confidential information will be available to the public through a variety of means, one of which will be the provisions of the Freedom of Information Act 2000.

Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

The availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience. This is supported by appropriate business continuity plans.

[1] The Data Protection Legislation are The Data Protection Act (1998), which is superseded by the and the EU General Data Protection Regulation from May 25th 2018 onwards

The BSO will:

- establish procedures and arrangements for handling queries from service users and members of the public
- undertake or commission regular assessments and audits of IG policies and arrangements
- ensure that non-confidential information about the organisation and its services is readily and easily available through a variety of media, in line with the ICO's model publication scheme
- proactively use information to support care, in compliance with the legislation and codes of practice issued by relevant regulators and DoH best practice.

4.2 Legal Compliance

All identifiable personal information is classified as confidential, except where national policy on accountability and openness requires otherwise.

The BSO will:

- establish and maintain policies and procedures to ensure compliance with Data Protection legislation, Human Rights Act 1998, the common law duty of confidentiality, Environmental Information Regulations 2004, and the Freedom of Information Act 2000
- treat all identifiable personal information as confidential
- develop and maintain the appropriate registers and systems to permit its functions as a data controller, and to act as a shared controller where this is required
- establish and maintain policies and procedures for the controlled and appropriate sharing of service user information, taking account of relevant legislation.

4.3 Information Security

BSO is dedicated to the secure management and use of information held, and compliance with the legislation and codes of practice issued by relevant regulators and the DoH in respect to information security.

The BSO will:

- establish and maintain an Information Security Policy along with respective procedures for effective policing and secure management of all information assets and resources
- 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 permanent/temporary, contracted staff, agency workersand third party associates adhere to this via appropriate laid down policy procedures, training and information awareness schemes/documentation

4.4 Information Quality Assurance

Data can be defined as a collection of text, figures or statistics which can be translated and processed into information. Information quality is a measurement of the robustness and usefulness of that data for its intended purpose. Information quality is fundamental to providing sound information to support business decision making processes and underpinning all activities and actions.

The BSO will:

- establish and maintain policies for information quality assurance and the effective management of records
- ensure that information we hold, through business arrangements, is of the highest quality in terms of completeness, accuracy, relevance, accessibility, timeliness and intelligibility
- ensure that managers are required to take ownership of, and seek to improve the quality of information within their functional areas and that information quality is assured at the point of collection
- undertake or commission regular assessments and audits of our 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

All information assets and information flows should be risk assessed to determine appropriate, effective and affordable IG controls are in place

Risk assessment in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, cost-effective IG controls are in place.

4.6 Records Management

Records management is a discipline to manage the creation, control, distribution, retention, storage and disposal of records. The underlying principle is to ensure that a record is managed through its life cycle from creation or receipt, through maintenance and use to disposal.

The BSO will:

- establish and maintain policies for effective records management
- promote records management through policies, procedures and training

4.7 Training

Awareness and understanding of all staff, with regard to their responsibilities, will be routinely assessed, recorded and appropriate training and awareness provided.

The BSO will ensure that:

- all staff complete mandatory training at induction, and on a two yearly cycle thereafter
- All staff have access to relevant IG policies and procedures.

5 Responsibilities

5.1 The **Board** has overall responsibility to ensure compliance in all areas of information governance.

5.2 The **Chief Executive** has ultimate responsibility for the delivery of this policy and subsequent policies and procedures.

5.3 The **Personal Data Guardian (PDG)** is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.

5.4 The **Senior Information Risk Officer (SIRO)** is an executive who has responsibility to ensure compliance with legislation through the development and monitoring of policy and codes of practice, and the appointment of Information Asset Owners (IAOs).

5.5 Information Asset Owners (**IAOs)** are senior individuals involved in running the relevant business area within each organisation. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and the use of those assets. The IAO should:

- know who has access to the asset and why
- ensure access is monitored and auditable
- understand, measure and address risks to the asset and provide assurance to the SIRO

5.6 **Information Asset Administrators (IAAs)** ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date. The IAA will be a member of operational staff responsible for one or more information assets as nominated by the IAO for the area of responsibility.

5.7 The BSO Data Protection Officer (DPO) is the designated **Information Governance Lead (IGL)** Key responsibilities include:

- ensuring there is senior level awareness and support for IG
- providing direction in formulating, establishing and promoting IG in the organisation
- drafting ,reviewing, revising, distributing and implementing IG policies
- monitoring and reporting on performance
- ensuring that the annual IMAC and improvement action plans are prepared for approval
- developing appropriate training for staff
- liaising with the ICO as required

5.8 All **Directors** are responsible individually and collectively for the application of the Information Governance suite of policies within their Directorates.

5.9 **Managers** are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance with the standards set out in the documents that make up the IG Framework.

5.10 **Managers** must also ensure that this policy and its supporting standards and guidelines are conveyed to their staff and any third party contractor working in the area and that there is on-going compliance with the standards set out in the documents that make up the IG Framework. They must also ensure that staff are adequately trained and apply the appropriate guidelines.

5.11 All **Staff** members, whether permanent, temporary or agency workers are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

5.12 **Information Governance Management Group (IGMG)**

The BSO operates an internal group (IGMG).

Each Directorate/Service area within the BSO should identify a representative ideally at Band 7 or above as an Information Governance Lead (IGL) to work as part of the BSO's IGMG and to be responsible for the coordination of IG compliance within their service area. A member of staff of a lower grade can be appointed as the IGL following consultation with the BSO SIRO.

The group will:

- ensure the development of an information governance culture within BSO.
- ensure the development of a comprehensive Corporate Information Asset Register
- develop policies and procedures to assist in the protection and safe use of information within BSO
- ensure the compliance within the organisation of all aspects of the IG Policy
- review policies in relation to IG on a regular basis
- develop support arrangements and provide staff with appropriate training and support to enable them to discharge their responsibilities to consistently high standards
- develop action plans to ensure on-going improvements in the management of IG within BSO
- maintain an overview of incidents affecting IG and security
- identify training and development requirements for staff within BSO in respect of IG

6 Performance and Monitoring Compliance

The effectiveness of this policy will be assessed on a number of factors:

- compliance with legislation
- the management (including frequency) of data breaches including inappropriate release of information, including near misses
- the retention, disposal and destruction of records in accordance with GMGR
- performance against IMAC on an annual basis
- staff training records.

7 Non-Compliance

A failure to adhere to the policy and its associated procedures/guidelines may result in disciplinary action and /or dismissal. Any breach of policy will be investigated and disciplinary action may be taken regardless of whether organisational equipment or facilities are used for the purpose of committing the breach. 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.

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

8 Review

This policy and all associated documents within the Information Governance Framework will be reviewed no later than two years from approval, to ensure their continued relevance to the effective management of information governance within the BSO.

9 Equality Statement

In accordance with the BSO's Equal Opportunities Policy, this policy will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, background or any other personal characteristic.