Business Services Organisation

Data Protection and Confidentiality Policy

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

Reference No:

Title:	BSO Data Protection and Confidentiality 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.	2.0	Supersedes:	1.0
Key Words:	Data Protection, Confidentiality, Responsibility		
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 Governance Policy		
	Information Security Policy		
	Information Risk Policy		
	Records Management Policy		
	Policy for the reporting of adverse incidents, accidents, near misses and dangerous occurrences		
	Policy for the Safeguarding, Movement and Transportation of Records, Files and Other Media		
	Freedom of Information Policy		

Contents

1. Introduction

1.1 Background

The Business Services Organisation (BSO) needs to collect personal information about people with whom it deals with in order to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. In addition, we may be required by law to process and share personal information with other organisations (including, but not limited to, police, regulatory and health and social care bodies).

As a public body, BSO has a statutory duty to safeguard the information it holds, from whatever source, which is not in the public domain. The lawful and proper treatment of personal information by BSO is extremely important to the success of our business and in order to maintain the confidence of our service users and employees.

1.2 Data Protection Principles

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

(a) processed lawfully, fairly and in a transparent manner;
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
(d) accurate and, where necessary, kept up to date;
(e) 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;
(f) 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.

1.3 Supporting Legislation

This policy has been written to support staff in compliance with legal requirements and best practice guidance, which includes but is not limited to:

- General Data Protection Regulation (GDPR) 2016
- Common Law duty of confidentiality
- Computer Misuse Act 1990
- Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order 1925
- Access to Health Records (Northern Ireland) Order 1993
- Human Rights Act 1998
- Crime and Disorder Act 1998

- Electronic Communications Act 2000
- Public Interest Disclosure Act 1998
- The Investigatory Powers Act 2016
- Guidance from the Information Commissioner's Office
- The Department of Health (DoH) Good Management, Good Records (GMGR)
- DoH Code of Practice on protecting the confidentiality of service user information (2012)

2. Purpose

The purpose of this policy is to lay down the principles that must be observed by anyone who works for, or on behalf of, BSO and has access to personal information.

This policy aims to clarify how and when personal information may be shared, and the need to make individuals aware of the ways in which their information might be used.

3. Scope

The scope of this policy is to support the protection, control and management of personal information. The policy will cover all information within BSO and is concerned with all information systems, electronic and non-electronic information. 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 BSO.

This includes, but is not necessarily limited to information:

- stored on computers, paper and electronic structured records systems;
- transmitted across internal and public networks such as email or Intranet/Internet;
- stored within databases;
- printed or handwritten;
- 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;
- 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.

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.

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

4. Definitions

4.1 Personal Information

The term 'personal information' applies to any information relating to an identified or identifiable natural person. It relates to both electronic and manual information held in any format.

4.2 Special categories of personal information

Article 9 of GDPR defines 'special categories' of personal information as information relating to:

- 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.

This policy should be read alongside the Information Governance Policy and ICT Security Policy, which deal with the security of information held by BSO and give important guidance in this respect.

4.3 Data Controller

The 'data controller' is defined as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal information.

4.4 Data Processor

A '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.

5. Objectives

BSO will apply the above principles to the management of all personal information by adopting the following policy objectives:

5.1 Privacy by design

BSO will apply 'privacy by design' when developing and managing information systems containing personal information by:

- Using proportionate privacy impact assessment to identify and mitigate data protection risks at an early stage of project and process design for all new or updated systems and processes;
- Adopting data minimisation: BSO will collect, disclose and retain the minimum personal information for the minimum time necessary for the purpose(s) that it is being processed; and
- Anonymising personal information wherever necessary and appropriate, for instance when using it for statistical purposes.

5.2 Fair and Lawful Processing

BSO will:

- Only collect and use personal information to the extent that it is needed to fulfil operational or legal requirements, and in accordance with the conditions set down under GDPR, namely:
    - Consent of the Data subject
    - To perform in terms of a contract
    - To comply with a legal obligation
    - To protect a data subject's vital interests
    - If it is in the public interest
- Provide transparent information on how personal information will be processed by way of 'fair processing notice', which will detail:
    - What information is needed
    - Why this information is needed
    - The purpose(s) that this information will be used for
    - How long this information will be kept for
- Ensure that personal information is collected for specific purpose(s), and will not be reused for a different purpose that the individual did not agree to or expect
- Ensure the quality of personal information processed

5.3 Disclosure of Personal Information

Strict conditions apply to the disclosure of personal information both internally and externally. BSO will not disclose personal information to any third party unless it is lawful to do so. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:

- we have the statutory power or are required by law to do so; or
- the information is clearly not intrusive in nature; or
- the individual has consented to the disclosure; or
- the information is in a form that does not identify the individual.

5.4 Right of Access

GDPR gives any individual who has personal information kept about them by BSO the right to request in writing a copy of the information held relating to them. BSO will ensure that an applicant receives access within a calendar month, unless there is a valid reason for delay or an exemption is applicable.

For further information, please refer to BSO's procedure for processing requests for information.

5.5 Safeguarding Information

BSO will ensure appropriate technical and organisational security measures are in place to safeguard personal information so as to prevent loss, destruction or unauthorised disclosure. For further information and guidance, please refer to the following policies:

- Information Security Policy
- Information Risk Policy

5.6 Retention and Disposal

GDPR places an obligation on the BSO not to keep personal information for longer than is required for the purpose(s) for which it was collected. Personal information will be disposed of by means that protect the rights of those individuals, and as such BSO will:

- Apply retention policies to all personal information;
- Destroy information no longer required in a secure manner; or
- Transfer the information, by arrangement, to the Public Records Office of Northern Ireland (PRONI) where deemed appropriate.

5.7 Uphold Individual's Rights

BSO will ensure that the rights of the individual under GDPR are upheld, where applicable, namely:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The rights in relation to automated decision making and profiling.

6. 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 personal information.

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

5.5 The **Data Protection Officer (DPO)** is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

5.6 All **Directors** are responsible individually and collectively for the application of the information governance suite of policies within their directorates.

5.7 The **Head of Corporate Services (HoCS)** is responsible for ensuring compliance with FOI requirements.

5.8 **Managers** are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes.

5.9 All **staff** members, whether permanent, temporary or agency 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. Staff are expected to:

- Familiarise themselves with, and abide by, the principles set out within this policy;
- Understand how to safeguard personal information.

5.10 Any **third parties** who are users of personal information processed by the BSO will be required to confirm and demonstrate that they will abide by the requirements of GDPR.

6 Performance and Monitoring Compliance

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

- Nomination of an individual or individual with specific responsibility for data protection within the BSO;
- compliance with legislation in respect of GDPR;
- the management of data breaches, including near misses;
- the retention and disposal of records in accordance with GMGR;
- performance against agreed standards on an annual basis;

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 2 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 characteristics