

POLICY DOCUMENT

Data Protection and Confidentiality Policy

Policy Review Schedule

Date first Approved: 12 September 2006

Last Approved by the Board: April 2018

Date of Next Review: April 2020

Policy Owner: Governance, IT & Facilities Manager

Amendment Overview

| Version | Date | Pages | Comments | Actioned |
|-----------------------|------------|-------|---|---------------------------------|
| 2006 - 1.0 | 12/09/2006 | | Policy created and agreed | Roisin Campbell |
| 2009 - 2.0 (Draft) | 31/03/2009 | | Policy updated to reflect role of IT & Records Management Officer. Accountability section added, and document formatted to comply with NIMDTA template. | Margot Roberts / Mark Oliver |
| 2009 - 2.0 | 18/06/2009 | | Presented to NIMDTA Board for re-approval | |
| 2009 - 2.0 | 04/08/2009 | | Re-issued to staff | |
| 2011 - 3.0 (Draft) | 12/08/2011 | | Policy re-drafted in line with Data Protection Policy Statement issued by DHSSPS | Mark Oliver |
| 2011 - 3.0 | 15/09/2011 | | Policy approved by NIMDTA Board with minor amendment. | |
| 2011 – 3.1 | 20/08/2013 | 17 | Role of NIMDTA to be included at beginning of each policy and corporate document. Footer updated to include new NIMDTA mission statement | Linda Craig |
| 2014 – 4.0 | 18/02/2014 | | Policy reviewed and updated | Mark Oliver |
| 2014 – 4.0 | 25/02/2014 | 17 | Presented to G&R Committee for approval. Approved subject to a minor change on Page 12. | |
| 2014-4.1 | 27/02/2014 | 17 | Presented to NIMDTA Board for approval. | |
| 2014-4.1 | 11/03/2014 | 17 | Presented to Extra-Ordinary meeting of NIMDTA Board for approval. Approved subject to minor changes. | |
| 2016 – 5.0 | 12/01/2016 | 10 | Identification of additional | Mark Oliver |

| | | | | |
|------------|------------|-----|--|--------------|
| | | | Information Asset Owners | |
| 2016 – 5.0 | 21/01/2015 | | Presented to Governance and Risk Committee for re-approval | |
| 2016 – 5.1 | 26/02/2016 | | Amended following G&R. Disciplinary Procedure added to “Policy Impact” section. Amendment to introduction. | Mark Oliver |
| 2016 – 5.1 | 28/04/2016 | | Presented to NIMDTA Board for re-approval. Approved | Mark McCarey |
| 2017 – 6.0 | 11/01/2017 | | Policy Reviewed and Updated following retirement of Administrative Director | Gillian Kerr |
| 2017 – 6.1 | 25/01/2017 | | Amended following G&R, in preparation for Board approval. Approved. | Gillian Kerr |
| 2018 – 7.0 | 29/03/2018 | ALL | Regionally developed policy adopted and amended to suit NIMDTA. | Mark Oliver |
| 2018 – 7.0 | 26/05/2018 | | Presented to NIMDTA Board for approval. Approved. | |

Contents

| | |
|---|----|
| Policy Review Schedule | 2 |
| Role of the Northern Ireland Medical and Dental Training Agency | 5 |
| Executive Summary | 6 |
| Policy Influence..... | 7 |
| Policy Impact | 7 |
| 1. Introduction | 8 |
| 1.1 Background | 8 |
| 1.2 Data Protection Principles | 8 |
| 1.3 Supporting Legislation | 9 |
| 2. Purpose | 9 |
| 3. Scope | 10 |
| 4. Definitions..... | 11 |
| 4.1 Personal Information | 11 |
| 4.2 Special categories of personal information | 11 |
| 4.3 Data Controller | 12 |
| 4.4 Data Processor..... | 12 |
| 5. Objectives | 12 |
| 5.1 Privacy by design | 12 |
| 5.2 Fair and Lawful Processing | 13 |
| 5.3 Disclosure of Personal Information..... | 13 |
| 5.4 Right of Access | 14 |
| 5.5 Safeguarding Information | 14 |
| 5.6 Retention And Disposal | 14 |
| 5.7 Uphold Individual's Rights | 15 |
| 6. Responsibilities | 15 |
| 6 Performance and Monitoring Compliance | 16 |
| 7 Non-Compliance | 17 |
| 8 Review..... | 17 |
| 9 Equality Statement..... | 17 |

Role of the Northern Ireland Medical and Dental Training Agency

The Northern Ireland Medical and Dental Training Agency (NIMDTA) is an Arm's Length Body sponsored by the Department of Health (DoH) to train postgraduate medical and dental professionals for Northern Ireland. NIMDTA seeks to serve the government, public and patients of Northern Ireland by providing specialist advice, listening to local needs and having the agility to respond to regional requirements.

NIMDTA commissions, promotes and oversees postgraduate medical and dental education and training throughout Northern Ireland. Its role is to attract and appoint individuals of the highest calibre to recognised training posts and programmes to ensure the provision of a highly competent medical and dental workforce with the essential skills to meet the changing needs of the population and health and social care in Northern Ireland.

NIMDTA organises and delivers the recruitment, selection and allocation of doctors and dentists to foundation, core and specialty training programmes and rigorously assesses their performance through annual review and appraisal. NIMDTA manages the quality of postgraduate medical and dental education in HSC Trusts and in general medical and dental practices through learning and development agreements, the receipt of reports, regular meetings, trainee surveys and inspection visits. It works in close partnership with local education providers to ensure that the training and supervision of trainees support the delivery of high quality safe patient care.

NIMDTA recognises and trains clinical and educational supervisors and selects, appoints, trains and develops educational leaders for foundation, core and specialty medical and dental training programmes throughout NI.

NIMDTA is accountable to the General Medical Council (GMC) for ensuring that the standards set by the GMC for medical training, educational structures and processes are achieved. The Postgraduate Medical Dean, as the 'Responsible Officer' for doctors in training, has a statutory role in making recommendations to the GMC to support the revalidation of trainees. Revalidation is the process by which the GMC confirms that doctors are up to date and fit to practice. NIMDTA also works to the standards in the COPDEND framework for the quality development of postgraduate Dental training in the UK.

NIMDTA enhances the standard and safety of patient care through the organisation and delivery of relevant and valued career development for general medical and dental practitioners and dental care professionals. It also supports the career development of general medical practitioners and the requirements for revalidation through the management and delivery of GP appraisal.

NIMDTA aims to use the resources provided to it efficiently, effectively and innovatively. NIMDTA's approach to training is that trainees, trainers and educators should put patients first, should strive for excellence and should be strongly supported in their roles.

Executive Summary

We need to collect and use information about people with whom we work in order to carry out our business and provide our services. These may include members of the public, current, past and prospective employees and trainees, customers and suppliers. In addition, we may be required by law to collect and use information. All personal information, whether in paper, electronic or any other format, must be handled and managed in accordance with Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR).

Policy Influence

This policy has been influenced by the following:

- General Data Protection Regulations
- Data Protection Act 1998
- 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) 1923
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Equality Act 2010
- 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
- DoH Code of Practice on Protecting the Confidentiality of Service User Information (2012)

Policy Impact

This policy may have an impact on the following:

- Freedom of Information Policy
- Information Requests Procedure
- Freedom of Information Publication Scheme
- Processing and Sharing of Information Relating to Doctors and Dentists
- IT Policy
- Records Management Strategy
- Disciplinary Procedure

1. Introduction

1.1 Background

The Northern Ireland Medical and Dental Training Agency (NIMDTA) needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include doctors and dentists in training, trainers, general practitioners (medical and dental), dental care professionals, 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, NIMDTA 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 NIMDTA 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

NIMDTA, 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 Regulations
- Data Protection Act 1998
- 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) 1923
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Equality Act 2010
- 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
- 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, NIMDTA and have access to personal information.

This policy aims to clarify how and, when personal information may be shared, 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 NIMDTA 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 staff, and as appropriate to contractors and third party service providers acting on behalf of NIMDTA.

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, NIMDTA and any individual directly employed or otherwise used by NIMDTA.

4. **Definitions**

4.1 **Personal Information**

The term 'personal information' applies to any data 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 Information Security Policy, which deal with the security of information held by NIMDTA 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 data.

4.4 Data Processor

A 'data processor' is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller.

5. Objectives

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

5.1 Privacy by design

NIMDTA 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
- Adopt data minimisation: NIMDTA will collect, disclose and retain the minimum personal information for the minimum time necessary for the purpose(s) that it is being processed
- Anonymise personal data wherever necessary and appropriate, for instance when using it for statistical purposes

5.2 Fair and Lawful Processing

NIMDTA 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. NIMDTA 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 data kept about them by NIMDTA the right to request in writing a copy of the information held relating to them. NIMDTA 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 NIMDTA's procedure for processing requests for information.

5.5 Safeguarding Information

NIMDTA 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 NIMDTA 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 NIMDTA will:

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

5.7 Uphold Individual's Rights

NIMDTA 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. At NIMDTA the Chief Executive also fulfils the role of **Personal Data Guardian (PDG)** - a senior person responsible for protecting the confidentiality of personal information.
- 5.3 The **Governance, IT and Facilities Manager** is responsible for ensuring compliance with FOI requirements.
- 5.4 The **Data Protection Officer (DPO)** is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements, under the terms of an SLA with the BSO.

- 5.5 The **IT and Records Management Officer (ITRMO)** is responsible for advising Heads of Department, Managers and staff locally within NIMDTA.
- 5.5 All **Heads of Department** are responsible individually and collectively for the application of the Information Governance suite of policies within their Department.
- 5.6 **Managers** are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes.
- 5.7 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:
- Familiarize themselves with, and abide by, the principles set out within this policy
 - Understand how to safeguard personal information
- 5.8 Any **third parties** who are users of personal information processed by NIMDTA 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 NIMDTA;
 - 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 NIMDTA.

9 Equality Statement

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