

Northern Ireland



Medical & Dental Training Agency

Policy

Data Protection

September 2011

Version 3.0

Contents

Introduction.....	2
Policy Influences.....	2
Policies Impacted.....	2
Statement of Policy.....	3
Data Protection Principles.....	3
Disclosure of Personal Information	4
Handling of Personal Information.....	4
Compliance.....	5
Accountability.....	5
Staff Responsibilities.....	6
Disposal and Retention of Personal Data	6
Sensitive Personal Data.....	7
Incoming and Internal Mail.....	8
Data Subject Rights and Access to Personal Data	8
Third Party Users of Personal Information	9
Policy Awareness	9
Policy Review Schedule.....	10

Introduction

The Northern Ireland Medical & Dental Training Agency (“the Agency”) is fully committed to complying with the Data Protection Act 1998 (DPA) which came into force on 1 March 2000.

We will follow procedures to ensure that all employees, contractors, agents, consultants and other parties who have access to any personal information held by or on behalf of us are fully aware of and abide by their duties and responsibilities under the Act.

Policy Influences

This policy has been influenced by:

- Data Protection Act 1998
- HSSPS Code of Practice on Protecting the Confidentiality of Service User Information
- Freedom of Information Act 2000
- Draft DHSSPS Data Protection Policy Statement

Policies Impacted

The following may be impacted by a change to this Policy:

- FOI Procedures Manual
- FOI Charging Policy
- Processing and Sharing of Information Relating to Doctors and Dentists
- IT Security Operating Procedures
- Records Management Policy
- Records Management Disposal Schedule
- Records Management Strategy
- Agency Publication Scheme

Statement of Policy

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 DPA.

Data Protection Principles

We fully support and comply with the eight principles of the Act. In summary, this means personal information must be:

- (i) processed fairly and lawfully;
- (ii) processed for limited purposes and in an appropriate way;
- (iii) relevant and sufficient for the purpose;
- (iv) accurate;
- (v) kept for as long as is necessary and no longer;
- (vi) processed in line with individuals' rights;
- (vii) secure;
- (viii) only transferred to other countries that have suitable data protection controls.

Our purpose for holding personal information, along with a general description of the categories of people and organisations to which we may disclose it, are listed in the [Information Commissioner's Data Protection Register](#).

Disclosure of Personal Information

Strict conditions apply to the disclosure of personal information both internally and externally. We will not disclose personal information to any third party unless we believe it is lawful to do so. Respect to confidentiality will be given where appropriate. 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.

Handling of Personal Information

All staff will, through appropriate training and responsible management:

- fully observe conditions regarding the fair collection and use of personal information;
- meet our legal obligations to specify the purposes for which personal information is gathered and used;
- collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of personal information used;
- apply strict checks to determine the length of time personal information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the Act;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without adequate safeguards.

Compliance

We will ensure that:

- there is always someone with specific responsibility for Data Protection in the organisation;
- all Subject Access Requests (SARs) will be dealt with in accordance with the Data Protection Act and within the 40 day time limit;
- each year staff are reminded of their obligations under DPA;
- everyone managing and handling personal information understands that they are directly and personally responsible for following good Data Protection practice;
- only staff who need access to personal information as part of their duties are authorised to do so;
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information is appropriately supervised;
- anyone wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- a regular review and audit is made of the way personal information is managed;
- methods of handling personal information are regularly assessed and evaluated;
- performance on handling personal information is regularly assessed.

Accountability

To assist in achieving compliance, we have:

- nominated the Chief Executive as Personal Data Guardian within the Agency, with the overall duty to ensure that the Agency complies with legislation affecting the handling of personal data and with supporting regulations and codes of practice;
- nominated the Administrative Director as the Senior Information Risk Owner (SIRO) within the Agency;

- nominated the Corporate Governance Manager as the Information Asset Owner (IAO) within the Agency;
- appointed an IT and Records Management Officer who provides assistance and support to departments on issues relation to data protection

Staff Responsibilities

All staff have a responsibility to protect the personal information held by the Agency. They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- they are appropriately trained in the handling of personal information;
- paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- personal data held on computers and computer systems is protected by the use of secure passwords which, where possible, have forced changes periodically;
- individual passwords are not easily compromised.
- personal data which they provide in connection with their employment is accurate and up-to-date, and that they inform the Agency of an errors, corrections or changes, for example, change of address, marital status, etc;

If and when, as part of their responsibilities, staff collect information about other people, they must comply with Data Protection legislation. No one should disclose personal information outside this legislation or use personal data held about others for their own purposes.

Unauthorised disclosure may be considered a disciplinary matter.

A blatant disregard of the policy will be subject to disciplinary action.

Disposal and Retention of Personal Data

The Data Protection Act 1998 places an obligation on the Agency to exercise care in the disposal of personal data, including protecting its

security and confidentiality during storage, transportation, handling, and destruction. All staff have a responsibility to consider safety and security when disposing of personal data in the course of their work. Consideration should also be given to the nature of the personal data involved (how sensitive is it?), and the format in which it is held.

The Data Protection Act also places an obligation on the Agency not to hold personal data for longer than is necessary. The Agency's Records Management Disposal Schedule advises on the procedures for disposing of records and the length of time records should be retained by the Agency.

Sensitive Personal Data

The 1998 Act introduces a new category of sensitive personal data, which is subject to additional safeguards.

Sensitive personal data is any personal data, which includes information on:

- racial or ethnic origin,
- political opinions, religious or similar beliefs,
- trade union membership,
- physical or mental health,
- sexual life,
- the (alleged) commission of any offence, subsequent proceedings or sentence.

Sensitive personal data should normally only be processed if the data subjects have given their explicit (written) consent to this processing. (explicit consent, is consent that refers to specific and identifiable processing of personal data. Such consent should where possible be obtained in writing as this can be used for future reference, whilst explicit verbal consent cannot). If this is not possible, the data may still be processed if one of a number of other conditions is met. The Agency, may process sensitive personal data without the subjects' explicit consent if the processing is necessary:

- Because of any right or obligation imposed by employment law.
- For medical purposes, including medical research, and is undertaken by a health professional or equivalent person.

- For equal opportunities monitoring and in compliance with Section 75 of the Northern Ireland Act 1998.

Sensitive personal data must be protected with a higher level of security and sensitive records should be kept separately in a locked drawer or filing cabinet, or in a password-protected computer file.

Incoming and Internal Mail

The following principles should be applied to the processing of incoming and internal mail:

- Paper-based mail that is marked 'Personal', or 'Private and Confidential', or which appears to be of a personal nature, should only be opened by the addressee, or a designated person. Unless paper-based mail items are marked in this way it will be assumed that they do not contain personal or confidential information.
- Any other mail will be assumed not to contain confidential information, as designated by the 1998 Act.
- Staff should not use their Agency address for anything other than Agency business.

Data Subject Rights and Access to Personal Data

All data subjects have the right to access any personal data that is being kept about them either on computer or in certain structured manual files. Any person who wishes to exercise this right should make their request in writing, to the Agency's Data Protection Co-ordinator. When making such a request, the individual must:

- Provide a suitable means of identification.
- Tell the Data Protection Co-ordinator where they believe the information is held.

The Agency reserves the right to charge the recommended administrative fee, currently £10; on each occasion that access is requested. The Agency aims to comply with requests for access to personal data as quickly as possible, but will ensure that it is provided within the statutory period defined in the 1998 Act.

The Agency does not have to give you any information, which identifies someone else, unless that person agrees. If you think that information might be held about you, which may identify another person, you may want to get that person's agreement to you being shown the information, and enclose that with your application.

Data subjects also have the right to:

- Require the Agency to ensure that no significant decisions that affect them are based solely upon an automated decision-taking process.
- Prevent processing likely to cause damage or distress.
- Prevent processing for the purposes of direct marketing.
- Take action for compensation if they suffer damage by any contravention of the 1998 Act by the Agency
- Take action to rectify, block, erase or destroy inaccurate data.
- Request the Information Commissioner to make an assessment, as to whether any part of the 1998 Act has been contravened.

Third Party Users of Personal Information

Any third parties who are users of personal information supplied by the Agency will be required to confirm and demonstrate that they will abide by the requirements of the Act. There will be an expectation that these parties will audit their compliance with the DPA and will provide assurances to the Agency in this respect.

Policy Awareness

All new and existing staff have access to this policy on the CETIS system, where they must read and provide acceptance. A copy of this policy statement will be given to interested third parties. Existing staff and any relevant third parties will be advised of any changes to the policy which will be posted on CETIS and made available on the Internet. All staff and relevant third parties must be familiar with and comply with this policy at all times.

Policy Review Schedule

Date first Approved: 12/09/2006

Last Approved by the Board: 15/09/2011

Date of Next Review: September 2013

Amendment Overview

Version	Date	Pages	Comments	Actioned
1.0	12/09/2006		Policy created and agreed	Roisin Campbell
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 Agency template.	Margot Roberts / Mark Oliver
2.0 (Draft)	18/06/2009		Presented to Agency Board for re-approval	
2.0	04/08/2009		Re-issued to staff	
3.0 (Draft)	12/08/2011		Policy re-drafted in line with Data Protection Policy Statement issued by DHSSPS	Mark Oliver
3.0	15/09/2011		Policy approved by Agency Board with minor amendment.	