

National Museum of Ireland

Data Protection - Code of Practice

DATE APPROVED: 4 February 2010	APPROVED BY: Board of NMI
IMPLEMENTATION DATE:	DIVISION RESPONSIBLE: Administration
DOCUMENT CODE:	VERSION NO: 002 - June 2011
NUMBER OF PAGES: 10	REVIEW DATE: June 2012

Contents

Introduction.....	2
Data Protection Officer /Coordinator.....	2
Types of Data held at the NMI - Personal Data.....	2
Code of Practice - Data Protection Rules.....	4
NMI staff members' Responsibilities	6
Audit of Data Protection and Code of Practice Procedures within the NMI.	6
Protocol for Reporting Breaches.....	6
Appendix 1 - Definitions.....	7
Appendix 2 – Enforcement of Data Protection Legislation.....	8
Appendix 3 – Defined Policy.....	9
Appendix 4 – Data Protection Officer/Coordinator.....	10

Introduction

The National Museum of Ireland (NMI) is committed to a policy of protecting the rights and privacy of individuals (including visitors, providers of goods/services, staff and others) in accordance with the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. The NMI requires, for administrative purposes, to process personal data about its staff, visitors, suppliers and other individuals with whom it has dealings. To comply with the law, personal data will be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

This Data Protection Policy is a statement of the NMI's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts of 1988 and 2003.

In order that data gathered and processed within the NMI is compliant with the Data Protection legislation, NMI's Code of Practice ensures that each staff member is aware of:

- the concept of Data Protection
- his/her responsibilities under the Data Protection Acts, 1988 and 2003

Data Protection Officer /Coordinator

The Human Resources Manager is the Data Protection Officer in the NMI. In addition, there are nominated Data Protection Co-ordinators who are responsible for all personal data held in the relevant Department/Unit. These co-ordinators report to the Data Protection Officer. A list of these Data Protection Co-ordinators is attached at Appendix 4.

Types of Data held at the NMI - Personal Data

Personal data relates to an individual who is or can be identified, either from the data, or from the data in conjunction with other information, that is in (or is likely to come into) the possession of the Data Controller. The Personal Data held in the NMI includes, but it is not exclusive to that outlined below:

Administration Division

- Personal information relating to staff members.
Name, address, e-mail address, telephone number, PPS number, training record, CV, date of birth, increment/PMDS information, details of next-of-kin, dependant(s), superannuation information and bank information.
- Personal information relating to recruitment.
Name, address, e-mail address, telephone number, and CV.
This information is held for one year from the competition date and then all information is disposed of in a secure manner.
- Personal information relating to the Board members.

Name, address, e-mail address, telephone number, PPS number, and bank information.

- Personal information relating to suppliers of goods and services.
Information received during procurement process such as name, address, e-mail address, telephone number, referees, and bank information.
- Personal information relating to general correspondence.
Name, address, e-mail address, and telephone number.

Collections Division

- Personal information relating to volunteers, interns, transition year students.
Name, address, e-mail address, telephone number, PPS number, training record, CV, date of birth, details of next-of-kin, dependant(s), referees, name of school/education institution, and name of supervisor/teacher.
- Personal information relating to suppliers of goods and services.
Information received during procurement process such as name, address, e-mail address, telephone number, referees, and bank information.
- Personal information relating to excavation licenses and licenses to export/alter artefacts.
Name, address, e-mail address, and telephone number.
- Personal information relating to donations and acquisitions under Section 1003 of the Taxes Consolidation Act.
Name, address, e-mail address, and telephone number.
- Personal information relating to offences and prosecutions under the National Monuments Acts.
Data held legitimately as a body with a statutory remit under the Acts and access is limited by the Data Protection Act 1988, section 5, (1), (a).
Name, address, e-mail address, information received during investigation/reports.
- Personal information relating to general correspondence.
Name, address, e-mail address, and telephone number.

Services Division

- Personal information relating to volunteers, interns, transition year students.
Name, address, e-mail address, telephone number, PPS number, training record, CV, date of birth, details of next-of-kin, dependant(s), referees, name of school/education institution, and name of supervisor/teacher.
- Personal information relating to suppliers of goods and services
Name, address, e-mail address, telephone number, information received during procurement process such as referees, and bank information.

- Personal information relating to the marketing and education operations such as visitors, education institutions (schools/colleges), tour operators Name, address, e-mail address, telephone number, training record, CV, date of birth, details of next-of-kin, and dependant(s), referees.
- Personal information relating to NMI's Photography Department – Image Bank Signed consent forms, name, address, e-mail address, and telephone number.
- Personal information relating to general correspondence. Name, address, e-mail address, and telephone number.

Code of Practice - Data Protection Rules

The NMI administers its responsibilities under the relevant legislation covered by the rules outlined below. The NMI will ensure that it:

- 1. Obtains and processes information fairly.***
- 2. Keeps data for specified, explicit and lawful purposes.***
- 3. Will use and disclose data only in ways compatible with the purpose for which it was obtained.***

Personal information obtained by the NMI for a particular purpose is not used for any other purpose, other than that for which it was obtained. This personal data is not divulged to a third party unless it is entirely 'compatible' with the specified purpose.

For the purposes of the Acts, the transfer of personal data to agents who are carrying out operations upon the data itself, on behalf of the NMI, and not retaining it for their own purposes do not constitute disclosures. Examples of such transfers might include the transfer of staff data to a separate payroll company for payroll administration purposes. Such a transfer of information will be covered by an appropriate contract under the Data Protection Acts.

- 4. Will keep data safe and secure.***

The NMI implements a high standard of physical and technical security by ensuring:

- Access to information is restricted in accordance with the Defined Policy (Appendix 3);
- ICT systems are password protected;
- Information on computer screens and paper files are hidden from callers to offices;
- Personal data is protected by strong encryption when being stored on portable devices or transferred electronically (including e-mail);
- Personal data is not stored on portable devices except in essential circumstances. Where deemed essential, the data will be encrypted and a record kept of the nature and extent of the data and why it is being stored on a portable device. Instructions/guidelines are in place to fully delete the data on the portable device when it is no longer being used;
- Appropriate facilities are in place for the disposal of confidential waste;
- Non-disclosure of personal security passwords to any other individual (including other employees within the organisation);
- Premises are kept secure at all times, especially when unoccupied;

- Audit logs are kept in relation to read access, changes, additions, and deletions to ICT programmes and systems;
- Appropriate data protection and confidentiality clauses are used in arrangements with any processors of personal data on the NMI's behalf, including:
 - Conditions under which data may be processed.
 - Minimum-security measures that the data processors to have in place.
 - Mechanisms or provisions that will enable the Data Controller to ensure that any data processor is compliant with the security practice including a right of inspection or an independent audit.

The Data Protection Officer will arrange for the above responsibilities to be assigned to the Data Protection Coordinators in each of the NMIs Department/Unit. The Data Protection Officer will conduct periodic reviews of the measures and practices in place.

5. *Keep data accurate, complete and up-to-date.*

The NMI complies with this requirement by ensuring that:

- The general requirement to keep personal data up-to-date is fully implemented;
- The manual and ICT procedures are adequate to ensure high levels of data accuracy;
- The appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date;
- The procedures are in place to ensure personal data held is accurate including reviewing records on a regular basis; identifying areas where errors are most commonly made and providing training to eliminate those errors;
- Each individual has a right to have any inaccurate information rectified or erased. Procedures relating to the accuracy of data is outlined in the Defined Policy (Appendix 3).

6. *Ensure that data is adequate, relevant and not excessive.*

The NMI ensures that the information sought and retained is the minimum amount needed for the specified purpose. This is subject to periodic review to assess the continued need for information sought.

7. *Retain data for no longer than necessary for the purpose(s) for which it is acquired.*

The NMI must ensure that staff members are clear about the length of time data will be kept and the reason why the information is being retained. The NMI's Defined Policy outlines the different types of data held (Appendix 3). As a Scheduled Body under the National Archives Act 1986, the NMI may retain, indefinitely, data relating to persons associated with the acquisition of museum artefacts and other functions of the institution as part of its permanent archive.

8. *On request, provide a copy of personal data to the relevant individual.*

The NMI has procedures in place to ensure that Data Subjects can exercise their rights to acquire personal data under the Data Protection legislation (Appendix 3)

NMI staff members' Responsibilities

- All NMI staff members have a duty to ensure compliance with the principles of Data Protection and must undertake to follow the provisions of this Code of Practice in accordance with the NMI's policy and procedures.
- All staff members are charged with the responsibility of ensuring that all data that they gather, access, manage and control, as part of their daily duties, is carried out in accordance with the Data Protection Acts and this Code of Practice.
- Staff members found in breach of the Data Protection rules may be found to be acting in breach of or, in certain circumstances, committing an offence under the Data Protection Acts, 1988 and 2003.
- All current and former staff members of the NMI, are accountable in relation to all data processed managed and controlled by them during the performance of their duties in the organisation.

Audit of Data Protection and Code of Practice Procedures within the NMI.

Internal Auditors will have responsibility for monitoring the NMI practices and procedures to ensure compliance in accordance with the Data Protection Acts, 1988 and 2003.

Protocol for Reporting Breaches

The relevant Data Protection Coordinator is responsible for his/her area for reporting:

- Any breaches of the NMI's Code of Practice.
- Any breaches of the regulations in the Data Protection Acts.

Such breaches are to be reported to the Data Protection Officer. The Data Protection Officer will then notify the Office of the Data Protection Commissioner.

Appendix 1

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the Code of Practice

Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All the NMI staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to staff members of the NMI and individuals who interact with the NMI.

Data - Information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Relevant Filing Systems - Any set of information organised by name; PPS number; payroll number; staff number; date of birth or any other unique identifier are all considered relevant.

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller.

Access Request – this is where a person makes a request to the organisation for the disclosure of his/her personal data under section 4 of the Acts.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data.
- Collecting, organising, storing, altering or adapting the data.
- Retrieving, consulting or using the data.
- Disclosing the data by transmitting, disseminating or otherwise making it available.
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment. This might mean, for example, an employee of an organisation to which the data controller out-sources work. The Data Protection Acts places responsibilities on such entities in relation to their processing of the data.

Appendix 2

Enforcement of Data Protection Legislation

Data Protection Commissioner

The Data Protection Acts established the independent office of the Data Protection Commissioner. The Commissioner is appointed by Government and is independent in the performance of his/her functions. The Data Protection Commissioner's function is to ensure that those who keep personal data in respect of individuals comply with the provisions of the Data Protection Acts. The Commissioner maintains a register, available for public inspection, giving general details about the data handling practices of a range of data controllers, such as Government Departments, state agencies and financial institutions. The Data Protection Commissioner has a wide range of enforcement powers to assist in ensuring that the principles of Data Protection are being observed. These include the serving of legal notices compelling a data controller to provide information needed to assist his enquiries, compelling a data controller to implement a provision in the Act, etc. The Data Protection Commissioner also investigates complaints made by the general public in relation to personal data and has wide powers in this area. For example, the Commissioner may authorise officers to enter premises and to inspect personal information held on computer or relevant paper filing system. Members of the public who wish to make formal complaints may do so by writing to the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlinton, Co. Laois, or by email to info@dataprotection.ie.

Where employees of the organisation, in the normal course of their duties, become aware that an individual including employees of the organisation may be in breach of the Acts, they should report the matter to the Human Resources Manager. A data controller found guilty of an offence under the Acts can be fined amounts up to €100,000 on conviction and/or may be ordered to delete all or part of a database if relevant to the offence.

Advice/Assistance

All requests for advice and assistance on data protection issues within the organisation should be directed to the Human Resources Manager

Applying for Access to Personal Data

Requests for personal data should be made, in writing, to the Human Resources Manager.

Responding to Requests

When a valid request is received, the NMI must reply within 40 days¹, even if personal data is not held.

¹ Data Protection Acts 1988 and 2003

Right to establish existence of personal data.

An individual who believes that a person keeps personal data shall, if s/he so requests the person in writing

a) be informed by the person whether s/he keeps any such data, and

(b) if s/he does, be given by the person a description of the data and the purposes for which they are kept, as soon as may be and in any event not more than 21 days after the request has been given or sent to her/him.

Appendix 3

Defined Policy

- The NMI ensures through its Data Protection Co-ordinators that personal data kept in all its Departments/Units is safe and secure, and adheres to the guidelines set out in the NMI's Data Protection Policy in keeping data safe and secure.
- Data Subjects who are NMI staff members can interact with the NMI to ensure accuracy of data by contacting the Data Protection Officer. The Data Protection Officer will put the requester in contact with the relevant Data Protection Co-ordinator.
- Data Subjects who are not NMI staff members can interact with the NMI to ensure accuracy of data by adhering to procedures set out in the NMI's Freedom of Information Act, 1997 and the Freedom of Information (Amendment Act) 2003, Section 15 and Section 16 Reference Book – see the NMI website www.museum.ie.
- Each Data Protection Coordinator in the relevant Department/Unit will ensure that personal data is retained no longer than is necessary, for the purposes for which it is acquired, and that data is adequate relevant and not excessive.
- The Data Protection Officer ensures Data Subjects who are NMI staff members can exercise their rights under Data Protection legislation
- The Data Protection Officer ensures Data Subjects who are not NMI staff members can exercise their rights under Data Protection legislation by keeping the NMI in line with the latest Data Protection legislation

Appendix 4

Data Protection Officer/Co-ordinators

The NMI Data Protection Officer – Human Resources Manager

ADMINISTRATION DIVISION

Data Protection Co-ordinator

Human Resources – HR Administrator (EO)
Finance – Finance Officer (HEO)
ICT – ICT Manager
Country Life - (EO)

COLLECTIONS DIVISION

Data Protection Co-ordinator

Art and Industry – Keeper
Irish Antiquities – Keeper
Irish Folklife – Keeper
Natural History – Keeper
Registration –Registrar
Conservation – Head of Conservation

SERVICES DIVISION

Data Protection Co-ordinator

Marketing – Head of Marketing
Education – Head of Education
Facilities – Facilities Manager
Photography – Senior Photographer
Design – Senior Graphic Artist

Useful Contacts

Data Protection Commissioner's Office,
Phone: 1890 252231,
<http://www.dataprotection.ie>
info@dataprotection.ie