POLICY:		Data Protection Policy & Procedures

FIRST DRAFT:		

ADOPTED:		BR 2013#02

AMENDMENTS:		

REVIEW:		June 2018

MIC Data Protection Policy

Policy Statement

All policies, guidelines and protocols of Mary Immaculate College, will reflect the Colleges commitment to the promotion of equality and will be fully compliant with the provisions of prevailing equality legislation.

Mary Immaculate College (MIC) is committed to protection of the rights and privacy of individuals (including students, staff and others) whose personal information is held by the College. This commitment is underpinned by full compliance with the statutory measures that ensure these rights, namely the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. The College has put in place a range of systems and procedures, which it reviews on a regular basis, in order to protect these rights.

Purpose of the Policy

In order to carry out its core functions, MIC needs to collect and use personal data (information) about its staff, students and other individuals who come into contact with the College. The College needs to process such data for purposes that include the organisation and administration of courses, the conducting of examinations, pursuit of research activities, recruitment and payment of staff, compliance with statutory obligations, etc. The College is legally obliged to safeguard the privacy rights of individuals in relation to the processing of their personal information for such purposes. The Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 provide for this by conferring rights on individuals as well as responsibilities on those persons processing personal data. Personal data, both automated and manual, are 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.

Key Terms & Definitions

In order to comply with legislation and to give clarity about its role and responsibilities in relation to data protection, MIC recognises the following terms and

definitions, as specified in the legislation:

- **Data** means information in a form that can be processed. It includes both automated data and manual data.
- **Automated data** means any information on computer, or information recorded with the intention that it be processed by computer.
- **Manual data** means information that is recorded as part of a relevant filing system or with the intention that it form part of a system.
- **Relevant filing system** means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.
- **Personal data** means data, including sensitive personal 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 College.
- **Sensitive personal data** relates to specific categories of data, which are defined as data relating to a person's racial origin; political opinions or religious or philosophical beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.
- **Data Controller** is a body that processes information about living people. The data controller must be in a position to control the contents and use of a personal data file.
- **Data Processor** is a body that processes personal data on behalf of a data controller
- **Data Subject** is an individual who is the subject of personal data
- **Processing** means performing any operation or set of operations on data,
  - comprising:
  - obtaining, assembling, organising and storing data,
  - using, consulting and retrieving data,
  - altering, erasing and destroying data,
  - disclosing data.

The Eight Rules of Data Protection

MIC undertakes to perform its responsibilities under the legislation in accordance with the following eight stated Data Protection principles as outlined in the Acts:

- **Obtain and process information fairly:**

  MIC obtains and processes personal data fairly and in accordance with its statutory and other legal obligations.

- **Keep it only for one or more specified, explicit and lawful purposes:**

  MIC keeps personal data for purposes that are specific, lawful and clearly stated. Personal data will only be processed in a manner compatible with these purposes.

- **Use and disclosure only in ways compatible with these purposes:**

  MIC only uses and discloses personal data in circumstances that are necessary for the purposes of for which it collects and keeps the data.

- **Keep it safe and secure:**

  MIC takes appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of data and against accidental loss or destruction.

- **Keep it accurate, complete and up-to-date:**

  MIC operates procedures that ensure high levels of data accuracy, completeness and consistency.

- **Ensure it is adequate, relevant and not excessive:**

  Personal data held by MIC are adequate, relevant and not excessive in data retention terms.

- **Retain for no longer than is necessary:**

  MIC has a policy on retention periods for personal data.

- **Give a copy of his/ her personal data to that individual, on request:**

  MIC has procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation.

Roles & Responsibilities

MIC has overall responsibility for ensuring compliance with Data Protection legislation

when it is the Data Controller of personal data. However, all employees and students of MIC who separately collect and/or control the content and use of personal data are individually responsible for compliance with the legislation.

The Information Compliance Office provides support, assistance, advice and training to all departments and offices to ensure that they are in a position to comply with the legislation. The office has responsibility for coordination and compliance relating to all data protection matters, including responding to general queries and requests by Data Subjects relating to **personal data** as well as requests for assistance from College employees involved in collecting, storing and processing personal information.

Procedures & Best Practice Guidelines

There are clear procedures in place at MIC for the collection, processing and maintenance of personal information required by the College to carry out its core functions. This policy is supplemented by a more detailed document, the MIC Data Protection Procedures and Best Practice Guidelines that set out these procedures in order to raise general awareness of the systems and procedures that are in place and also to assist MIC employees to comply with the College's Data Protection Policy and the relevant legislation. The MIC Data Protection Procedures and Best Practice Guidelines identify the areas of work in which Data Protection issues arise, and outline best practice in dealing with these issues.

This Procedures and Best Practice Guidelines are available on the College website. It is also available on request from the Information Compliance Office or *dataprotection@mic.ul.ie*.

Queries:

Any queries relating to data protection issues, including requests by individuals for access to and/or correction of any personal data held by the College and relating to such individuals should be directed as follows:

Information Compliance Office
Mary Immaculate College, South
Circular Road,

Limerick
Tel: +353-61-204511
E-mail:dataprotection@mic.ul.ie

Review

This Policy will be reviewed at 5-year intervals in line with MIC protocols. The Policy may be reviewed between such intervals in the event of any legislative or other relevant developments.

Data Protection Policy

Appendix 1: Procedures

MIC Data Protection Procedures

Introduction

In its Data Protection Policy, MIC sets out the following:

> Mary Immaculate College (MIC) is committed to protection of the rights and privacy of individuals (including students, staff and others) whose personal information is held by the College. This commitment is underpinned by full compliance with the statutory measures that ensure these rights, namely the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003.

In order to protect these rights, the College has put a range of systems and procedures in place. These systems and procedures are subject to regular review in response to any legislative or other relevant developments that may occur.

This document sets out these procedures in order to raise general awareness of the ways in which it meets these commitments and also to provide all MIC employees involved in the collection, processing and maintenance of personal information required by the College to carry out its core functions with guidelines to assist them to comply with the College's Data Protection Policy and the relevant legislation.

Key Principles

As specified in the data protection legislation and outlined in the MIC Data Protection Policy, there are 8 "rules of data protection" which must be observed in order to ensure effective compliance. These rules are as follows:

- **Obtain and process information fairly**
- **Keep it only for one or more specified, explicit and lawful purposes**
- **Use and disclosure only in ways compatible with these purposes**
- **Keep it safe and secure**
- **Keep it accurate, complete and up-to-date**
- **Ensure it is adequate, relevant and not excessive**
- **Retain for no longer than is necessary**
- **Give a copy of his/ her personal data to that individual, on request**

Roles & Responsibilities

Certain key definitions need to be understood in order to reach clarity about roles and responsibilities relating to data protection policy. The Office of the Data Protection Commissioner provides such definitions and MIC adheres to these in ensuring compliance:

- **Data** means information in a form that can be processed. It includes both automated data and manual data.
- **Automated data** means any information on computer, or information recorded with the intention that it be processed by computer.
- **Manual data** means information that is recorded as part of a relevant filing system or with the intention that it form part of a system.
- **Relevant filing system** means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.
- **Personal data** means data, including sensitive personal 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 College.
- **Sensitive personal data** relates to specific categories of data, which are defined as data relating to a person's racial origin; political opinions or religious or philosophical beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.
- **Data Controller** is a body that processes information about living people. The data controller must be in a position to control the contents and use of a personal data file.
- **Data Processor** is a body that processes personal data on behalf of a data controller
- **Data Subject** is an individual who is the subject of personal data
- **Processing** means performing any operation or set of operations on data, comprising:

» obtaining, assembling, organising and storing data,

» using, consulting and retrieving data,

» altering, erasing and destroying data,

» disclosing data.

The Associate Vice President Administration (see contact details, below) has responsibility for coordination and compliance relating to all data protection matters, including general queries and the processing of requests by data subjects relating to **personal data**.

Other Relevant College Policies and Procedures

Data protection issues have relevance within a variety of settings and these guidelines should be read by staff and other interested parties in conjunctions with related policies and procedures that have been put in place by MIC. These policies and procedures include:

- Data Protection Policy
- Records Retention Schedule
- FOI procedures (Section 15 Manual)
- Privacy Policy
- Policy for Responsible Computing
- MIC Research Ethics Committee (MIREC) policies and procedures
- Child Protection Guidelines
- Procedures for Complaints by a Student
- MIC Text Alert Service Protocol

All of these policies and procedure are available on the College website (*www.mic.ul.ie*) or may be requested from the Associate Vice President Administration.

Data Protection Procedures

Data protection procedures in operation at MIC are categorised under headings consistent with the "8 Rules":

Obtaining and processing personal data

Personal data is obtained fairly if the data subject is aware of the purpose for which the College is collecting the data, of the categories of person/organisation to whom the data may be disclosed, of non-obligatory or optional answers in forms, of the right of access to the data and of the right of rectification of the data.

- Obtain personal data only when there is a clear purpose for so doing, obtain only whatever personal data are necessary for fulfilling that purpose and ensure data are used only for that purpose.
- The use of College data processing facilities in capturing and storing personal data for non-business purposes must not take place.
- Inform data subjects of what personal information is held by the College, what it will be used for and to whom it may be disclosed.
- Obtain explicit consent in writing for processing sensitive data and retain a copy of that consent. Consent cannot be inferred from non-response in the case of sensitive data.

Disclosing personal data

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data are kept. Special attention should be paid to the protection of sensitive personal data, the disclosure of which would normally require explicit consent.

- Except where there is a statutory obligation to comply with a request for personal data, or where a data subject has already been made aware of disclosures, do not disclose to any third party any personal data without the consent of the data subject.
- Verbal consent to disclosure of personal data to the data subject may be obtained by telephone in the case of non-sensitive personal data, but must include asking the subject to confirm facts that should be known only to them, such as date of birth, student number, etc. The date and time of the giving of the verbal consent should be recorded in writing.
- Verbal consent to disclosure of personal data to a third party is not permitted unless there is a statutory obligation to disclose, or the information is released, to the

Gardai for example, for the prevention of crime and if informing the subject of the disclosure would prejudice the enquiries, or unless it is in the vital interest of the data subject.

- Personal data should only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfil administrative functions. Be satisfied of the need to disclose.
- Personal data should not be disclosed outside of the EEA unless written consent has been obtained, unless disclosure is required for the performance of a contract to which the data subject is a party, or unless disclosure is necessary for the purpose of legal proceedings.

Permitted disclosures of personal data

The Acts provide for disclosures, where data are:

- authorised for safeguarding the security of the State;
- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- required to protect the international relations of the State;
- required urgently to prevent damage to health or serious loss/damage to property;
- required under law;
- required for legal advice or legal proceedings;
- disclosed to the data subject;
- disclosed at the request or with the consent of the data subject.

Securing personal data

The College must protect personal data from unauthorised access when in use and in storage and such data must be protected from inadvertent destruction, amendment or corruption.

- Personal electronic data should be subject to appropriate stringent controls, such as passwords, encryption, access logs, backup, etc.
- Screens, printouts, documents, and files showing personal data should not be visible to unauthorised persons.

- Personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited access.
- Subject to the MIC Records Retention Schedule, personal manual data should be destroyed by confidential shredding when the retention period has expired.
- When upgrading or changing PC, ensure the hard drive is cleaned by an appropriate IT staff member.
- Special care must be taken where laptops and PCs containing personal data are used outside the College.
- Special care must be taken to ensure the safety and security of any personal data held on mobile storage media.
- Health and social work personal data can only be released following consultation with the relevant professional.
- Disclosing personal data to a Data Processor should be done only under a written contract specifying security rules to be followed.

Accuracy and completeness of personal data

Administrative procedures should include review and audit facilities so that personal data are accurate, complete and kept up-to-date.

Retention of personal data

Data should not be kept for longer than is necessary for the purpose for which they were collected. Data already collected for a specific purpose should not be subject to further processing that is not compatible with the original purpose. All data held by the College should be stored and catalogued in accordance with the Records Retention Schedule and destroyed in accordance with that schedule and in compliance with statutory obligations.

Disposal of personal data

Personal data should be disposed of when they are no longer needed for the effective functioning of the College and its members. The method of disposal should be appropriate to the sensitivity of the data. Shredding is appropriate in the case of manual data and reformatting or overwriting in the case of electronic data. Particular care should be taken

when PCs are transferred from one person to another or outside the College or are being disposed of.

Rights of data subjects

Right of access

The Data Protection Acts provide for the right of access by a Data Subject to his or her personal information.

Data subjects must be made aware of how to gain access to their personal data. A Data Subject is entitled to be made aware of his or her right of access and to the means by which to access the data. A Data Subject is entitled to the following on written application within forty days, or 60 in the case of examination data:

- A copy of his or her personal data;
- the purpose of processing the data;
- the persons to whom the College discloses the data;
- an explanation of the logic used in any automated decision-making;
- a copy of recorded opinions about him or her, unless given in confidence (in which the subject may have recourse to access under the Freedom of Information Acts, 1997 & 2003).

Any applicants or intending applicants for access to personal information under the Data Protection Acts should be advised that the College reserves the right to charge a retrieval fee. A maximum fee of €6.35 may be charged.

Restriction of rights of access

The right of access is restricted where the data are:

- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- subject to legal professional privilege;
- kept only for statistical or research purposes and the results are not made available in a way that identifies data subjects;
- back-up data.

Provision of access to third parties

A Data Subject is entitled to access his or her own personal data only. The personal

information of a Data Subject, including confirmation of attendance at the College or contact details, must not be disclosed to a third party, be they parent, potential employer, employer, professional body, sponsor, etc., without the consent of the individual concerned.

An agreement may be made to forward a communication to a Data Subject on behalf of a third party, but no information should be disclosed about the Data Subject. In the case of research surveys where there is an agreement to forward documentation to Data Subjects, a notice should be included to the effect that no personal information has been released.

Limitations on the use of personal data for research

All researchers, be they students or staff, involved in collecting personal data, especially sensitive personal data, must comply with the requirements of the Acts. Initially, they must ensure that data are obtained and processed fairly. It is essential that the necessary consent from Data Subjects is obtained. Whenever possible, personal data should be rendered anonymous.

The Acts require that personal data shall be kept only for one or more specified, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those. This restriction may limit the usefulness of data for research purposes. If personal data is made anonymous, however, it ceases to be personal data subject to the terms of the Acts.

It should be noted that if research data is retained in personally identifiable format it may be subject to an access request from a data subject and is subject to restrictions on the transfer of data outside the European Economic Area.

Research involving Data Subjects as defined in these guidelines must also comply with policies and procedures governed by the MIC Research Ethics Committee (MIREC)

Right of rectification or erasure

Data subjects have a right to have personal data rectified, or blocked from being processed or erased where the Data Controller has contravened the Acts.

In order to comply with the above rights of access, rectification or erasure, ensure that personal data can be located and collated quickly and efficiently:

- Ensure personal data is in a format that is easy to locate and collate;
- Verify that the access request and the personal data released refer to the same individual;
- Know exactly what data is held on individuals, and by whom;
- Hold personal data in a secure central location.

Responsibilities of Data Subjects

The College is dependent on Data Subjects themselves for maintaining the accuracy and currency of records held about them. The College cannot be responsible for any inaccuracies resulting directly from the submission of such information by Data Subjects nor can it be accountable for any subsequent changes to such information unless notified. All Data Subjects have the right to review personal information about themselves recorded and stored by the College and to have it amended if necessary. All Data Subjects (including staff, students and others) are entitled to be informed as to how their personal data can be kept up to date and accurate by the College.

- All staff, students and other data subjects are responsible for
- checking that any information that they provide to the College is accurate and up to date;
- informing the College of any changes of information, that they have provided, e.g. changes of address;
- checking the information the College sends out from time to time, giving details of information kept and processed;
- informing the College of any errors or changes (the College cannot be held responsible for any errors unless previously informed).

Queries

The Associate Vice President Administration has responsibility for coordination and compliance relating to all data protection matters, including responding to general queries and requests by Data Subjects relating to **personal data** as well as requests for assistance from College employees involved in collecting, storing and processing personal information.

For such assistance or further information, contact:

Information Compliance Office,
Mary Immaculate College, South
Circular Road,
Limerick
Tel: *+353-61-204332*
E-mail: *dataprotection@mic.ul.ie*