Hibernia College Quality Framework

Policy for Personal Data and Records

1 Introduction

1.1 Purpose

This policy sets out the principles and responsibilities of all members of the Hibernia College community in relation to the collection, storage, processing and retention of personal data. This policy relates to the use and processing of all personal data which identifies or is capable of identifying any living individual, and which therefore requires compliance with the European Union's General Data Protection Regulation ("**GDPR**")[1] and the Data Protection Acts 1988 – 2018 (the "**Acts**"). This policy should be read in conjunct with the College's Privacy Policy.

1.2 Scope

a. To whom does the policy apply?

i. This is an overarching policy setting out how personal data is processed by the College and applies to the processing of personal data by all staff, faculty, adjunct faculty, students and third parties.

b. In what situations does the policy apply?

i. This policy relates to all situations in which personal data is used and processed by the College.

c. Who is responsible for implementing the policy?

i. The Records and Data Manager is responsible for managing the College's implementation of the Policy for Personal Data and Records and for managing and addressing breaches of this policy.

ii. The Director of IT is responsible for operational matters regarding the technical security and safety of personal data.

iii. All staff, faculty, adjunct faculty and students have individual responsibility for ensuring that this policy is adhered to where personal data is being collected, stored, processed or retained for any purpose, including research collection.

iv. Any third parties involved in collaboration or contracted to complete work with the College for any reason are responsible for adhering to this policy.

[1] European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Accessed: 01 May 2020); Data Protection Act (2018) *Data Protection Act 2018*. Available at: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print.html (Accessed: 01 May 2020).

1.3 Definitions

The College adopts the following definitions, as appropriate.

a. *Data Controller*

A data controller is a person or body who determines the purposes and means of the processing of personal data. In this regard, the College is the Data Controller. However, this responsibility extends to all persons using and processing personal data in relation to their work or studies with the College, where those persons determine the purposes and means of the processing of personal data.

b. *Data Processor*

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

c. *Data Subject*

A data subject is an identifiable natural person who can be identified, directly or indirectly, from a dataset. As a data controller, the College and members of the College community are responsible for ensuring any processing of that personal data occurs in line with the principles at set out in this policy.

d. *Personal Data*

Personal data is information relating to an identifiable natural person who can be identified directly or indirectly from factors, such as name, contact details or any attributes distinguishing a person.

e. *Special Category Data*

Special Category Data is information relating to an identifiable natural person which requires a higher level of protection than personal data and includes personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

f. *Criminal Offence Data*

Criminal Offence Data is a type of data in its own right that can only be processed by an organisation that has legal authority to do so. This is information about criminal allegations, proceedings or convictions as outlined under Article 10 of the GDPR.

g. *Identifiable Natural Person*

An identifiable natural person is one who can be identified, directly or indirectly, from a source of data.

2 Context

2.1 Legal or Regulatory Context

The College will comply with all requirements with regard to its data protection obligations, including the following:

a. *GDPR*

This policy is intended to facilitate the College in fulfilling its obligations under GDPR. The GDPR is a regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

b. Irish Data Protection Law

This policy is also intended to ensure the College's compliance with the Acts.

c. QA Guidelines

The policy is designed to comply with both the European standards and guidelines[2] and QQI's Core Statutory QA Guidelines[3], which both specify requirements in respect of the collection, processing, storage and disposal of data.

3 Policy Statements

3.1 Principles for Data Processing

a. Collection and Processing of Data

i. The College only collects, uses and processes personal data in the following contexts:

- The data subject has provided consent to the processing of their personal data.
- Processing is necessary for the performance of a contract with the data subject or in order to take steps at the request of the data subject before entering into a contract.
- Processing is necessary to protect the vital interests of a data subject or another natural person.
- Processing is necessary to fulfil legal and accreditation obligations to which the College is subject.
- Processing is necessary for the purposes of the College's legitimate interests except where such interests are overridden by the fundamental rights of the data subject.

ii. The College endeavours to ensure that personal data is:

- Processed lawfully and fairly.
- Collected for specified purposes.
- Relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Retained for no longer than necessary.
- Processed in a manner that ensures appropriate security of personal data.

b. Storage

i. The College stores personal data and records in a format that is suitable for the processing of the personal data and records.

ii. The College ensures that personal data and records are stored in a safe and secure manner.

c. Retention

i. We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we

[2] European Association for Quality Assurance in Higher Education (ENQA) et al. (2015) *Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG)*, 2nd edn, p.32, Section 1.7). Available at: http://www.enqa.eu/wp-content/uploads/2015/11/ESG_2015.pdf (Accessed: 01 May 2020).

[3] Quality and Qualifications Ireland (2016) *Core Statutory Quality Assurance (QA) Guidelines*, Section 8. Available at: https://www.qqi.ie/Downloads/Core%20Statutory%20Quality%20Assurance%20Guidelines.pdf (Accessed: 01 May 2020).

consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

ii. Pleases see the College Document Retention Schedule for further information on retention periods.

d. Disposal

i. Where the relevant retention period has expired, all personal data is destroyed promptly and securely, and is permanently deleted from the College's system.
ii. A record is retained with regard to the disposal or destruction of personal data.

e. Support

i. The College provides support, assistance, advice and training to all departments, offices and staff to ensure that all parties are in a position to comply fully with this policy.

f. Criminal Offence Data

i. The College will only process criminal offence data in specific circumstances where it is required to do so in order to fulfil its obligations.
ii. Garda vetting information is collected as required under the Children and Vulnerable Persons Act and the College's Policy for Admission and Procedure for Garda Vetting.

g. Special Category Data

The College only processes special category data in specific circumstances as required to fulfil its legal obligations as a private unlimited company and as a higher education institution. This may include the following:

i. Data concerning health may be required to fulfil obligations and to provide evidence of personal circumstances as set out in College procedures, such as the Policy for Appeals and the Policy for Extenuating Circumstances.
ii. Any other data as required for processing of students' academic performance.

h. Exemptions for Research

Subject to the existence of appropriate safeguards, Article 89 of the GDPR sets out certain exemptions to the principles of data processing for research purposes. These exemptions are set out below, and the College may apply these exemptions with regard to personal data collected for research purposes, where necessary: -

i. **Storage Limitation:** Research data can be held for an indefinite period of time.
ii. **Purpose Limitation:** Research data can be used for a purpose other than that it was originally intended for, provided that purpose is still research.
iii. **Data Subject Rights:** Certain exemptions as are set out in Article 89 of the GDPR may apply with regard to data subject rights (set out below).

The above exemptions apply where not exercising these exemptions would prevent or seriously impair the research process or if the research process is unlikely to cause substantial damage or distress to an individual.

i. *Maintaining Accurate Records*

i. The College is required to maintain accurate and up-to-date records for any data subject for whom the College holds personal details, which includes both students and graduates.
ii. Changes to student and graduate personal details specifically are processed in line with the Procedure for Change of Personal Details.

3.2 Third Party Disclosure

a. Personal data will only be disclosed as needed:

i. to processers approved by and carrying out necessary functions for the College under criteria specified by the College;
ii. where the College is required to do so by law or by professional bodies in connection with the performance of a contract in respect of the data subject;
iii. to any department or appointed authorised person within the company or any member company within this group, which means any subsidiary or holding company within the meaning of sections 7 and 8 of the Companies Act 2014;
iv. to any governmental, financial or regulatory body, agency or department;
v. to business partners, suppliers and sub-contractors for the performance of any contract entered into with them or the data subject in relation to the services, including insurers and adjunct faculty;
vi. to research partners including participating schools, healthcare providers and/or higher education institutions in Ireland and abroad in relation to any project or placement you undertake or agree to participate in;
vii. to selected third parties including the Garda Vetting Unit and educational partners, including but not limited to Quality & Qualifications Ireland, the Teaching Council and the Nursing and Midwifery Board of Ireland, as well as other Professional, Regulatory or Statutory Bodies in connection with the performance of any contract we may enter into with you;

b. We will disclose your personal information to third party recipients:

i. if the College sells or buys any business or assets, personal data will be disclosed to the prospective seller or buyer of such business or assets;
ii. if the College, or substantially all of its assets, are acquired by or transferred to a third party whether in the event of a merger, reorganisation, transfer of undertakings, receivership, liquidation or other winding up or any other similar circumstances, in which case personal data held by the College will be one of the transferred assets;
iii. if the College is under a duty to disclose or share a data subject's personal data in order to comply with any law, legal obligation or court order, or in order to enforce rights under the law, our Terms and Conditions of Website Use or any other agreements;
iv. to protect our rights, property or safety, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of maintaining the security of the websites and services.

3.3 Rights of the Data Subject

a. Right of Access

i. Data subjects have the right to access a copy of their personal data under the Procedure for Managing a Data Access Request.

b. Right of Rectification

i. Data subjects have a right to have their records amended in the case of inaccuracies in, or actual changes to, their personal details.

c. Restriction of Processing

i. Data subjects have a right to restriction of processing of their personal data, except where processing is based on lawful grounds other than consent.

d. Right to Erasure

i. Data subjects have a right to have their personal details deleted, except where processing is based on lawful grounds other than consent.

e. Right to Portability

i. Where it is technically feasible, data subjects have the right to have an easily accessible copy of their personal data transferred or moved to another data controller, except where that processing is based on lawful grounds other than consent.

f. Right to Object

Data subjects have the right to object to processing or restrict processing of their personal data if:

i. The personal data is processed unlawfully.
ii. Restriction is needed to comply with legal obligations.
iii. The data subject has withdrawn consent.

3.4 Principles for Managing Data Subject Access Requests ("DSAR")

a. Timeframe of Response

i. All DSARs received by the College must be responded to within one month, irrespective of weekends and public holidays.
ii. The date of receipt of a DSAR is the date on which the DSAR was received by the College and this date is the beginning of the one-month period.
iii. Where a request is complex, or multiple requests are received from the same individual, the College can extend this time by a maximum of two months. Where an extension is sought, the data subject is notified within a one-month period and an explanation for why the extension is necessary.

b. Notification of Departments

i. Where a DSAR is received by the College, all relevant departments must be notified.
ii. Stakeholders will be notified about their responsibilities in assisting to identify categories of requested data.

c. Delivery of Request

i. Information will be sent securely via the format requested by the data subject.

d. Record of Request

i. A record of the DSAR will be retained for the purpose of auditing and evaluation.

e. Exemptions

i. Emails sent by students using a College email account are outside the scope of a normal DSAR unless there is data specific, identifiable and retrievable contained within and the data subject has an explicit legitimate interest for pursuing it.
ii. Research data cannot be obtained as part of a DSAR, except where requesting such data does not impair or prevent the research project.
iii. Where a subject data access request is considered manifestly unfounded or excessive by the College, having undertaken a detailed assessment, the College may refuse to act on the request in line with Article 12(5) of GDPR. If this is the case, the College will inform the data subject of its decision.

3.5 Principles for Managing Data Security breaches

a. Notification of the Data Protection Commission

i. The College as a data controller is obliged to respond promptly to an actual or potential data security breaches as outlined in the Procedure for Managing Personal Data Security Breaches.

ii. Where the breach presents a risk to the affected individuals, the College is required to notify the Data Protection Commission of such a breach within 72 hours of becoming aware of the breach.

iii. The notification will be made through the "Breach Notification Form" on the Data Protection Commission website and will include the nature of the personal data breach.

b. Notification of Relevant Stakeholders and the Data Subject

i. Where a breach is likely to result in a high risk to the affected individuals, the College must also inform those individuals without undue delay.

ii. Any stakeholders deemed relevant to the data breach will be notified.

c. *Records and Evaluation*

i. Records of all personal data breaches are maintained in line with the College retention schedule.

ii. Evaluation of practice is conducted regularly to ensure effective practice.

4 Document Control

Document Title	Policy for Data and Records		
Author	Records and Data Manager		
Version	V.1 V.2 V.2.1	Adoption Date	28/06/2018 15/09/2020 08/10/2020
Expected Review Date	Three years from adoption date		
Related Policies	Policy for Acceptable Use of ICT Policy for Public Information, Promotion and the Recruitment of Students		
Related Procedures	Procedure for Managing Personal Data Security Breaches Procedure for Managing a Data Subject Access Request (DSAR) Procedure for Change of Personal Details		
Related Resources	Document Retention Schedule HCQF Guidelines for Data Protection and the Handling of Student Data Guideline for Implementing Data Protection Principles in Research Privacy Policy		