Data Protection and the Handling of Student Data Guidelines

Section 1 - Introduction

Hibernia College and Student Personal Data

(1) Processing student data is an integral part of the day-to-day operation of Hibernia College. As a data controller, the College has an obligation to protect the data privacy, security and integrity of our data subjects, including our students, in line with the principles set out in the Personal Data and Records Policy.

Who are these guidelines for?

(2) These guidelines are to support any Staff, Faculty or Adjunct Faculty member in the implementation of data protection principles in their role and in the day-to-day handling of student data.

Section 2 - What Is Data Protection?

Data Protection Principles

(3) The following seven principles underpinning data protection are dealt with in the Personal Data and Records Policy :

a. Lawfulness, fairness and transparency
b. Purpose limitation
c. Data minimisation
d. Accuracy
e. Storage limitation
f. Integrity and confidentiality
g. Accountability

Definitions

(4) The following key data protection terms apply to this document:

a. Data Controller
b. Data Processor
c. Data Subject
d. Personal Data
e. Special Category Data
f. Criminal Offence Data
g. Identifiable Natural Person

Examples of Students' Personal, Special Category Data and Criminal Offence Data

(5) Examples of students' personal data held by Hibernia College includes but is not limited to:

a. Biographical information such as name, address, date of birth, PPS number, phone number and email address
b. Data relating to studies such as student number, prior educational data (i.e. grades achieved at leaving cert, grades achieved at third level), grades achieved during study, admissions data, academic appraisal and feedback
c. Emergency contact/next of kin

(6) Examples of Special Category Data

a. Certificates pertaining to a student's mental or physical health provided as evidence for absences, reasonable accommodation, assessment extensions and pause in studies

(7) Examples of Criminal Offence Data

a. Garda Vetting disclosures and associated information

Section 3 - Accessing Personal Data

(8) The GDPR gives individuals the right of access to their personal data. This includes the right to confirmation that personal data concerning them is being processed and the right to request a copy of any such data. These requests are often referred to as Data Subject Access Requests (DSARs).

(9) Data subjects have the right to access data pertaining to them in any format, including documents where they are identified directly or indirectly by any identifier such as a PPS number or student number or any attributes distinguishing a person.

(10) The College's process for dealing with a DSAR is set out in the Data Subject Access Request (DSAR) Management Procedure.

Section 4 - How Can You Ensure You Are Handling Student Data Appropriately?

Part A - Taking Care in Identifying Student Personal Details

Verifying Student Identity

(11) Hibernia College Staff, Faculty and Adjunct Faculty should take care to ensure they are responding to a student's official College email address, or students' email as registered with the College, in all written communications.

(12) When communicating with students on the phone, Staff, Faculty and Adjunct Faculty should ask two verification questions to verify the student's identity before releasing any personal information. The first verification question should always be a request for their Student Number. Additional questions can include verification of registered address, telephone number and date of birth.

(13) In instances where special category data is being requested, it may be appropriate to request the student to produce a copy of photographic identification in consultation with the Data and Records Office, e.g. students requesting records of data they submitted as evidence in a formal process, such as requests for extensions and

applications related to reasonable accommodations.

Cause for Concern for Student Identity

(14) Whenever there is uncertainty about a person’s identity, the Records and Data Manager must be contacted without delay.

(15) The Records and Data Manager will conduct an investigation and will notify all departments to hold all correspondence relating to the individual until their identity can be confirmed.

(16) In cases where there is any doubt as to whether a personal data security breach has occurred, the Records and Data Manager should be consulted immediately.

Change of Personal Details

(17) Students can submit a Change of Personal Details Application Form to the Data and Records Office to update or amend their personal details.

(18) Any requests received by other College Staff, Faculty and Adjunct Faculty should be forwarded to the Data and Records Office for processing.

Part B - Taking Care in Student Data Handling

Drafting Documentation

(19) Hibernia College Staff, Faculty and Adjunct Faculty should ensure that all documentation, records or correspondence which contain student data are drafted in consideration of the students’ right of access.

Unauthorised Use of Data

(20) Accessing student data for usage outside of your contract with Hibernia College is strictly prohibited. Such prohibited usage includes but is not limited to personal interests or commercial interests.

Confidentiality

(21) Hibernia College Staff, Faculty and Adjunct Faculty should never discuss any aspect of a student’s grade or academic record with another person outside of the College. This includes the parent, spouse or friend of a student. Our contract is with the student alone.

(22) If a student provides any Staff member with special category data, the Staff member should ensure that the special category data is passed to the appropriate Hibernia College Staff or Faculty member. Once the data has been passed to the appropriate person, the Staff member should permanently delete the data from their records.

Data Handling in Assessment

(23) When marking several assessments in a row, Hibernia College Staff, Faculty and Adjunct Faculty should ensure the file name matches the name and student number on the account to which the file is uploaded.

(24) Ensure that feedback files are not mixed up with personal files on your device.

(25) Do not save any assessment or feedback material to unsecure environments. This includes, desktops, unlicensed cloud services and USBs.

(26) Once you have concluded marking an assessment and you have received confirmation that the relevant data has

been received by the College, delete all information pertaining to the assessment from your device.

(27) Avoid paper records unless absolutely necessary.

Part C - Practising Good Data Security

Keeping Your Access to Hibernia College Systems Secure

(28) Ensure that your password to Hibernia College systems including, but not limited to, Outlook, Quercus, MyHELMS and Inplace is strong and secure. Use a mixture of lowercase, uppercase, letters, numbers and special characters. Do not use a password that is the same as a password you use in other contexts. Ensure that your password is regularly changed.

(29) Never allow another person to access the College information systems using your account.

(30) If you suspect your account has been compromised, change your password immediately and contact the Hibernia College Information Technology department.

(31) If you are accessing Hibernia College systems from a shared device, do not save your passwords.

Device Safety

(32) Never leave your device unattended without ensuring it is password protected. Never leave your device unattended in an unsecure location for any reason.

(33) Ensure your device is encrypted or password protected.

(34) To safeguard against cyber-attacks, viruses and malwares, ensure your device is equipped with an adequate firewall and anti-virus software.

(35) If your device is lost or stolen, contact the Records and Data Manager and the Information Technology department immediately.

Email Correspondence with Students

(36) When sending group emails, use MyHELMS wherever possible.

(37) If, for a legitimate reason, you are required to use email for group correspondence, always send group emails via the ‘bcc’ field, not the ‘to’ field. If students can view the contact details of their classmates, this is a data breach.

(38) Be very mindful when forwarding email threads from students as the content may contain protected or sensitive information that the subsequent recipient does not need to view or is not entitled to view.

Part D - Data Breaches

Discovering a Suspected Data Breach

(39) If you discover, or even suspect a data breach, consult the Personal Data Security Breach Management Procedure and contact the Records and Data Manager immediately at dpo@hiberniacollege.net

Breach Notifications

(40) Where the College has determined that the data breach is likely to result in a risk to the rights and freedoms of data subjects, the data breach must be reported to the Data Protection Commission within 72 hours of first having

become aware of the breach.

(41) Data processors are also required to notify their customers, the controllers, ‘without undue delay’ after first becoming aware of a data breach.

Examples of Data Breaches

(42) Examples of data breaches include:

a. Disclosing information about a student to another student
b. Disclosing information about a student to a person not contracted by Hibernia College to serve students
c. Publishing of student information on websites and social media
d. Inadvertently sending emails via reply all to those who did not need to view that information
e. Data is stolen by physical or electronic means

Part E - Questions or Concerns

(43) If you have any questions or concerns, feel free to contact the Records and Data Manager at dpo@hiberniacollege.net.

Status and Details

Status	Current
Effective Date	2nd November 2020
Review Date	2nd November 2023
Approval Authority	Academic Board
Approval Date	23rd September 2020
Expiry Date	Not Applicable
Enquiries Contact	Quality Assurance

Glossary Terms and Definitions

"Reasonable Accommodation" - 'A Reasonable Accommodation is any action that helps to alleviate a substantial disadvantage due to an impairment or medical condition.' (AHEAD). In the context of supporting higher education students, a reasonable accommodation is any provision made for a particular student to allow them to demonstrate their achievement of the learning outcomes of a piece of learning without any disadvantage which may arise on the basis of their having a disability or long-term illness.

"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.

"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.

"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.

"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.

"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.

"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.

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