Personal Data Security Breach Management Procedure

Section 1 - Introduction

Purpose and Parent Policy

(1) Under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), Hibernia College is obliged to keep personal data safe and secure and to respond promptly and appropriately in the event of a personal data security breach. This procedure lays out the steps to be followed by the College in the event that a personal data security breach or suspected personal data security breach occurs.
The Personal Data and Records Policy is the parent policy.

Responsibilities

Student Responsibilities

(2) Students have a responsibility to report any breach or suspected breach of personal data to the Data Protection Officer as soon as they become aware of such a breach at dpo@hiberniacollege.net.

Staff, Faculty and Adjunct Faculty Responsibilities

(3) The Data Protection Officer is responsible for this procedure.

(4) All Staff, Faculty and Adjunct Faculty are responsible for engaging with and adhering to, this procedure as required.

(5) All Staff, Faculty and Adjunct Faculty are responsible for reporting any breach or suspected breach of personal data to the Data Protection Officer without delay.

Section 2 - Procedure for Managing Personal Data Security Breaches

Part A - What is a data breach?

(6) A personal data security breach is any incident which gives rise to an unauthorised disclosure, loss, destruction or alternation of personal data held by the College in any format. This includes any breaches which result from malicious conduct, lack of appropriate security controls, system or human failure or error. Personal data security breaches can happen for a number of reasons, including:

a. The disclosure of confidential data to unauthorised individuals
b. Loss or theft of data or equipment on which data is stored
c. Loss or theft of paper records
d. Inappropriate access controls allowing unauthorised use of information

e. Attempts to gain unauthorised access to computer systems, e.g. hacking
f. Records altered or deleted without authorisation by the data 'owner'
g. Viruses or other security attacks on IT equipment systems or networks
h. Breaches of physical security, e.g. forcing of doors or windows into a secure room or filing cabinet containing personal data
i. Personal data viewable in accessible areas
j. Leaving IT equipment unattended when logged in to a user account without locking the screen to stop others accessing information
k. Emails containing personal or special category data sent in error to the wrong recipient

Part B - Identification and Initial Assessment of a Suspected Breach of Personal Data

Identification and Notification of Suspected Personal Data Security Breach

(7) Any individual who suspects that a personal data security breach has occurred, whether they have caused, been subject to or identified a breach of personal data, are required to:

(8) Immediately upon becoming aware of the breach, notify the Data Protection Officer at dpo@hiberniacollege.net, who will advise them on any required steps that need to be taken

(9) Notify their line manager (where applicable) without delay

(10) Complete the Personal Data Security Breach Report Form, available under the resources section of the Hibernia College Quality Framework, and forward to the Data Protection Officer as soon as possible

Initial Assessment

(11) The Data Protection Officer conducts an initial assessment as a matter of priority, which will include a review of:

a. The nature of the personal data involved in the breach (i.e. whether special category data is involved)
b. The cause of the breach
c. The extent of the breach (i.e. the number of data subjects affected)
d. The potential harm to which the affected data subjects may be exposed
e. Any steps that may be taken to contain the breach
f. Determining if any other College stakeholders need to be informed of the incident

Outcome of Initial Assessment

(12) Where the outcome of an initial assessment confirms that a personal data breach has not occurred, the process concludes, and the Data Protection Officer notifies the reporter that no data breach has occurred.

(13) Where the outcome of an initial assessment confirms that a personal data security breach has occurred, the Data Protection Officer will immediately proceed to coordinate the College response, as follows.

Part C - Managing a Confirmed Personal Data Security Breach

Containment and Recovery

(14) In the event of a confirmed personal data security breach, immediate and appropriate steps must be taken to mitigate the risks and limit the extent of the breach by the Data Protection Officer and, in consultation with any

relevant College Staff, will:

a. Identify Staff members within the College who need to be aware of the breach and inform them of their expected role in containing the breach
b. Establish and implement measures to address the risks created by the breach in conjunction with relevant Staff members
c. Inform the College Executive Management Team
d. Inform any outside agencies concerned, e.g. schools or hospitals, as appropriate
e. Undertake a risk assessment to consider the potential adverse consequences for the affected data subjects, including how likely such adverse consequences are to materialise and how serious or substantial they are likely to be
f. Assess the risks for the College to include strategic, operational, legal, financial and reputational risks, as appropriate
g. Where appropriate, inform the Gardaí (in cases involving criminal activity)

Risk Assessment

(15) As is set out above, where a personal data security breach is confirmed, the Data Protection Officer in conjunction with relevant College Staff, will conduct a risk assessment to assess the potential adverse consequences for the affected data subjects. The assessment will consider the likelihood of the risks taking place and the severity of such risks and will consider the following criteria:

a. Type of breach
b. Nature of the personal data
c. Scale and volume of the personal data affected
d. Ease of identification of the affected data subjects
e. Security measures in place
f. Containment measures
g. Severity of the risk
h. Likelihood of the risk(s) materialising

Notification of the Data Subject

(16) Where the personal data security breach is likely to result in a high risk to the rights and freedoms of the data subject, the College will inform the affected data subjects, without undue delay.

(17) Where it is necessary to notify the data subject, the Data Protection Officer will assist staff to communicate the details of the data breach to the data subject(s) to include the:

a. Name and contact details of the Data Protection Officer or other contact point where more information can be obtained
b. Likely consequences of the personal data security breach
c. Measures taken, or proposed to be taken, by the controller to address the personal data security breach, including, where appropriate, measures to mitigate its possible adverse effects

Notification of the Data Protection Commissioner

(18) Where the College has determined that the personal data security breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will notify the Data Protection Commission without undue delay, and no later than 72 hours, after becoming aware of the breach. If, for any reason, the breach cannot be

notified to the Data Protection Commission within 72 hours, the notification will be accompanied by reasons for the delay.

(19) The notification will include the nature of the personal data security breach, including the:

a. Categories and approximate number of data subjects concerned
b. Categories and approximate number of personal data records concerned
c. Name and contact details of the Data Protection Officer or other contact point where more information can be obtained
d. Likely consequences of the personal data security breach
e. Measures taken, or proposed to be taken, by the College to address the personal data security breach, including, where appropriate, measures to mitigate its possible adverse effects

Evaluation and Response

(20) The Data Protection Officer retains all records of the incident

(21) The Records and Data Manager, in consultation with all relevant stakeholders, will conduct a review of the incident to:

a. Ensure the steps taken during the incident were appropriate and effective
b. Identify any areas for improvement

(22) The review report is issued to all relevant departments.

(23) A post-incident review will be conducted to ensure that the steps taken during the incident were appropriate and effective and to identify any areas which may need to be improved in future to avoid any recurrence.

Status and Details

Status	Current
Effective Date	19th May 2023
Review Date	19th May 2026
Approval Authority	Quality Assurance Administrator
Approval Date	19th May 2023
Expiry Date	Not Applicable
Enquiries Contact	Eoin Crossen Quality Assurance Administrator Quality Assurance

Glossary Terms and Definitions

"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.