

Hibernia College Quality Framework

Procedure for Managing Personal Data Security Breaches



1 Introduction

1.1 Purpose and Parent Policy

Hibernia College, under Data Protection legislation, 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 if a breach of personal data is suspected.

The Policy for Data and Records applies.

1.2 Responsibilities

a. Student Responsibilities

- i. Students have a responsibility to report any suspected breach of their personal data to the Data and Records manager without delay.

b. Staff Responsibilities

- i. The Records and Data Manager has responsibility for the implementation of the procedure.
- ii. All staff are responsible for the execution of this procedure.

c. Faculty Responsibilities

- i. All faculty and adjunct faculty are responsible for the execution of this procedure.

2 Procedure for Managing Personal Data Security Breaches

2.1 Procedure one

a. Initial Steps where Personal Security Data Breach is suspected

- i. Contact the Records and Data Manager without delay.
- ii. Complete the Personal Data Security Breach Form and forward to the Records and Data Manager.

b. Identification and Initial Assessment

- i. The Records and Data Manager conducts an initial assessment to include:
 - The nature of the personal data involved in the breach (i.e. whether sensitive personal data is involved)
 - The cause of the breach
 - The extent of the breach (i.e. the number of individuals affected)
 - The potential damages to the Data Subjects
 - Any steps that may be taken to contain the breach

- Identify if any other Hibernia College stakeholders need to be informed of the incident.
- ii. Where no breach is confirmed, the process concludes and reporters are notified that no risk to data security has occurred.

c. Containment and Recovery

Where a breach is confirmed, the Records and Data Manager, in consultation with any relevant Hibernia College Staff, will:

- i. Establish staff members within Hibernia College who need to be aware of the breach and inform them of their expected role in containing the breach.
- ii. Establish and implement measures to ameliorate the damage caused by the breach in conjunction with relevant staff members.
- iii. Inform any outside agencies concerned, i.e., Schools or Hospitals as appropriate.
- iv. Undertake a risk assessment to consider the potential adverse consequences for individuals, including how likely such adverse consequences are to materialise and how serious or substantial they are likely to be.
- v. Assess the risks for Hibernia College to include strategic, operational, legal, financial, and reputational risks as appropriate.

d. Notification of the Data Subject

- i. The Records and Data Manager will communicate the details of the data breach to the Data Subject(s) to include:
 - the name and contact details of the Records and Manger or other contact point where more information can be obtained
 - the likely consequences of the personal data breach
 - the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

e. Notification of the Data Protection Commissioner

- i. The Records and Data Manager notifies the Data Protection Commissioner without undue delay and no later than 72 hours after the breach has been apparent.
- ii. The notification shall include the nature of the personal data breach including:
 - The categories and approximate number of data subjects concerned and
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the data protection officer or other contact point where more information can be obtained
 - The likely consequences of the personal data breach
 - the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

f. Evaluation and Response

- i. The Records and Data Manager retains all records of the incident.
- ii. The Records and Data Manager in consultation with all relevant stakeholder conducts a review of the incident to:
 - Ensure the steps taken during the incident were appropriate and effective
 - Identify any areas for improvement.
- iii. The report of the review is issued to all relevant departments.

3 Document Control

| | | | |
|----------------------|--|---------------|------------|
| Document Title | Procedure for Managing Personal Data Security Breaches | | |
| Author | Records and Data Manager | | |
| Version | V.1 | Adoption Date | 16/08/2018 |
| Expected Review Date | August 2019 | | |
| Related Policies | Policy for Data and Records | | |
| Related Procedures | | | |
| Related Resources | | | |