Personal Data Security Breach Management Procedures Version 1.0

The purpose of these procedures is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data held by the Institute. These procedures are a supplement to the Institute's Data Protection Policy which affirms the Institute's commitment to protect the privacy rights of individuals in accordance with Data Protection legislation.

Document Location Freedom of Information / DP Office

Revision History

Date of this revision: Compilation date 9 January 2017	Date of next review: 9 January 2019

Version Number/Revision Number	Revision Date	Summary of Changes
1.0	9 Jan 2018	
2.0	Aug 2017	

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
0.1	Jan 2017		1st draft of policy written
0.2	Aug 2017	FAR & GB	

Approval

This document requires the following approvals:

Name	Title	Date
Executive Board	Institute Management Team	28 April 2017
Finance Audit & Risk Committee	Governing Body	August 2017
Governing Body	Governing Body	August 2017

These procedures have been approved by the Institute Management. Any additions or amendments to this or related policies will be submitted by the Data Protection Officer for approval or to whatever authority Executive Board may delegate this role. These procedures will be reviewed annually by the Data Protection Officer who will consult as necessary before submitting any amendments for approval.

TABLE OF CONTENTS

1. INTRODUCTION

Dundalk Institute of Technology ("the Institute") is obliged under the Data Protection Acts, 1988 and 2003 (the "Data Protection Acts") and any subsequent legislation to keep personal data safe and secure and to respond promptly and appropriately to data security breaches (including reporting such breaches to the Data Protection Commissioner in certain cases). It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the Institute.

2. PURPOSE

The purpose of these procedures is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data (defined below) held by the Institute. These procedures are a supplement to the Institute's Data Protection Policy which affirms its commitment to protect the privacy rights of individuals in accordance with Data Protection legislation.

3. WHAT IS A PERSONAL DATA SECURITY BREACH?

A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by the Institute in any format. Personal data security breaches can happen for a number of reasons, including:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of data or equipment on which data is stored;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of the Institute's IT security and Acceptable Use policies;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- records altered or deleted without authorisation by the data "owner";
- viruses or other security attacks on IT equipment systems or networks;
- breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information
- confidential information left unlocked in accessible areas;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- emails containing personal or sensitive information sent in error to the wrong recipient.

4. WHO DO THESE PROCEDURES APPLY TO?

These procedures apply to all users of Institute data, including:

- any person who is employed by the Institute or is engaged by Institute who has access to Institute data in the course of their employment or engagement for administrative, research and/or any other purpose;
- members of Governing Body,
- any student of the Institute who has access to Institute data in the course of their studies for administrative, research and/or any other purpose;
- individuals who are not directly employed by DkIT, but who are employed by contractors (or subcontractors) and who have access to Institute data in the course of their duties for DkIT

hereinafter, collectively referred to as "**Members**".

5. WHAT TYPES OF DATA DO THESE PROCEDURES APPLY TO?

These procedures apply to:

- all personal data created or received by the Institute in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;
- personal data held on all Institute IT systems managed centrally by the IT Dept, and locally by individual Schools/Departments/Offices/Functions or Centres;
- any other IT systems on which Institute data is held or processed.

6. WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA SECURITY BREACHES?

Personal data security breaches are managed by the FOI Officer, Ms Loretto Gaughran on behalf of Data Protection Officer – Mr Peter McGrath, VP for Financial & Corporate Affairs in conjunction with the relevant Manager and Manager of IT Services (where appropriate).

In emergency situations, the Institute's **Critical Response Team** will take over responsibility for managing the incident (see section 8 below).

7. PROCEDURE FOR REPORTING PERSONAL DATA SECURITY BREACHES

In the event of a breach of personal data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

If a member of the Institute becomes aware of an actual, potential or suspected breach of personal data security, he/she must report the incident to their Head of Department/School/Office immediately.

The Head of Department/School/Office must then:

- **report the incident immediately to the FOI Officer/DP Officer: Extension 2631**
- **complete the attached Data Security Breach Report Form and email it to foi@dkit.ie as soon as possible.**

This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

8. PROCEDURE FOR MANAGING DATA SECURITY BREACHES

In line with best practice, the following five steps should be followed in responding to a data security breach:

Step 1: Identification and initial assessment

Step 2: Containment and Recovery

Step 3: Risk Assessment

Step 4: Notification

Step 5: Evaluation and Response

Step 1: Identification and initial assessment of the incident

If a member of the Institute considers that a data security breach has occurred, this must be reported immediately to the member's line manager/head of department who will in turn notify the **FOI Officer** **FOI@dkit.ie** . The line manager/head of department should complete part 1 of the Data Security Breach Report Form (Appendix 1) and return it to the FOI Officer without delay. Part 1 of the Report Form will assist the DP Officer/FOI Officer in conducting an initial assessment of the incident by establishing:

- if a personal data security breach has taken place; if so:
- what personal data is involved in the breach;
- the cause of the breach;
- the extent of the breach (how many individuals are affected);
- the harms to affected individuals that could potentially be caused by the breach;
- how the breach can be contained.

Following this initial assessment of the incident, the DP Officer/FOI Officer will, investigate the incident or appoint an investigator (e.g. IT Manager for IT-related incidents, etc.) and will decide if it is also necessary to appoint a group of relevant Institute stakeholders to assist with the investigation. Any records relating directly to an investigation will be retained by the DP Officer/FOI Officer.

The Lead Investigator (if appointed), liaising with the DP Officer/FOI Officer and the Head of the area affected by the breach, will determine the **severity** of the incident using the checklist in **Appendix 2** and by completing **part 2 of the Data Security Breach Report Form (Appendix 1)** (i.e. s/he will decide if the incident can be managed and controlled locally or if it is necessary to escalate the incident to the **Institute Crisis Management Team**). The severity of the incident will be categorised as level 1, 2a, 2b or 3.

Level 1 classed as a Local Incident
Level 2 (a) classed as a Minor Emergency Type (A) both managed and controlled locally

Level 2 (b) classed as Minor Emergency Type (B)
Level 3 classed as a Major Emergency Escalated to Crisis Management Team which

is responsible for the management and close out of the incident

Step 2: Containment and Recovery

Once it has been established that a data breach has occurred, the Institute needs to take immediate and appropriate action to limit the breach.

The Lead Investigator, liaising with the DP Officer/FOI Officer and relevant Institute staff members/managers, will:

- Establish who within the Institute needs to be made aware of the breach (e.g. IT Services, Estates Office, Legal/Insurance, Communications Office) and inform them of what they are expected to do to contain the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes on doors, etc.)
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause (e.g. physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data).
- Establish if it is appropriate to notify affected individuals immediately (e.g. where there is a high level of risk of serious harm to individuals).
- Where appropriate (e.g. in cases involving theft or other criminal activity), inform the Gardaí.

Step 3: Risk Assessment

In assessing the risk arising from a data security breach, the relevant Institute stakeholders are required to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. The information provided at Stage 1 on the Data Security Breach Report Form will assist with this stage.

The Lead Investigator and DP Officer/FOI Officer in conjunction with the head of department/unit/function/centre in which the incident occurred will review the incident report to:

- Assess the risks and consequences of the breach:
  - Risks for individuals:
    - What are the potential adverse consequences for individuals?
    - How serious or substantial are these consequences?
    - How likely are they to happen?
  - Risks for the Institute:
    - Strategic & Operational
    - Compliance/Legal
    - Financial
    - Reputational
    - Continuity of Service Levels
- Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

The Lead Investigator and DP Officer/FOI Officer will prepare an **incident report** setting out (where applicable):

- a summary of the security breach;
- the people involved in the security breach, (such as staff members, students, contractors, external clients);
- details of the information, IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;
- how the breach occurred;
- actions taken to resolve the breach;
- impact of the security breach;
- unrealised, potential consequences of the security breach;
- possible courses of action to prevent a repetition of the security breach;
- side effects, if any, of those courses of action;
- recommendations for future actions and improvements in data protection as relevant to the incident.

The incident report will then be furnished to the Head of School/Department/Function/Centre (as appropriate) affected by the breach. Such Heads will request relevant staff to update the risk registers at the appropriate levels where necessary. Any significant risks will be reported to the Risk Management Committee and addressed though the Institute's Risk / Crisis Management Policy and Emergency Plan.

Step 4: Notification

On the basis of the evaluation of risks and consequences, the DP Officer/FOI Officer, and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside the Institute. For example:

- the Gardaí;
- individuals (data subjects) affected by the breach;
- the Data Protection Commissioner;
- other bodies such as regulatory bodies, grant funders;
- the press/media;
- the Institute's insurers
- bank or credit card companies
- trade unions
- external legal advisers.

As well as deciding **who** to notify, the DP Officer/FOI Officer must consider:

- **What** is the message that needs to be put across?

  In each case, the notification should include as a minimum:

  - a description of how and when the breach occurred;
  - what data was involved;
  - what action has been taken to respond to the risks posed by the breach.

When notifying individuals, the DP Officer/FOI Officer should give specific and clear advice on what steps they can take to protect themselves, what the Institute is willing to do to assist them and should provide details of how they can contact the Institute for further information (e.g. helpline, website).

- **How** to communicate the message?

  What is the most appropriate method of notification (e.g. are there large numbers of people involved? Does the breach involve sensitive data? Is it necessary to write to each individual affected? Is it necessary to seek legal advice on the wording of the communication?).

- **Why** are we notifying?

  Notification should have a clear purpose, e.g. to enable individuals who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc.

In accordance with the Data Protection Commissioner's ***Personal Data Security Breach Code of Practice*** all incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner ("OPDC") as soon as the Institute becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) **and** it affects no more than 100 data subjects **and** it does not include sensitive personal data or personal data of a financial nature. In case of doubt – in particular any doubt related to the adequacy of technological risk-mitigation measures – the Institute should report the incident to the OPDC.

Any contact with the Data Protection Commissioner should be made through the DP Officer/FOI Officer. Initial contact with the OPDC should be made by the DP Officer/FOI Officer within **two working days** of becoming aware of the breach, outlining the circumstances surrounding the incident. This initial contact may be by e-mail (preferred by the OPDC), telephone or fax and must not involve the communication of personal data. The OPDC will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data. In cases where the decision is made by the Lead Investigator and DP Officer/FOI Officer not to report a breach, a brief summary of the incident with an explanation of the basis for not informing the Data Protection Commissioner will be retained by the DP Officer/FOI Officer.

NOTE: The Communications Office/Manager should be consulted prior to any media notice being issued.

Step 5: Evaluation and Response

Subsequent to a data security breach, a review of the incident by the DP Officer/FOI Officer in consultation with the relevant stakeholders in the Institute will take place to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

All data security breach reports should be sent to the DP Officer/FOI Officer who will use these to compile a central record (log) of incidents. The DP Officer/FOI Officer will report on incidents to the Executive Board at least on a quarterly basis in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed.

For each **serious** incident, (the Lead Investigator and) DP Officer/FOI Officer will conduct a review to consider and report to the Executive Board on the following:

- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Whether policies procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Are staff and users of services aware of their responsibilities for information security and adequately trained?
- Is additional investment required to reduce exposure and if so what are the resource implications?

9. RELATED POLICIES AND PROCEDURES

These procedures underpin the following Institute policies and procedures:

Data Protection Policy
Data Protection Procedures
How to Make an Access Request
Records Retention Schedule
DP Guidelines for Staff / Students
Data Governance Policies & Procedures
CCTV Policy 2014

DkIT staff should ensure compliance with the above policies and procedures in addition to these Data Breach Management Procedures.

10. FURTHER HELP AND ADVICE

For further information and advice about this procedure and about data protection matters, please contact:

Loretto Gaughran
DP Officer/FOI Officer
Human Resource Office
Dundalk Institute of Technology

Phone: (042) 93 70222
Email: foi@dkit.ie

11. DISCLAIMER

The Institute reserves the right to amend or revoke these procedures at any time without notice and in any manner in which the Institute sees fit at the absolute discretion of the Institute or the President of the Institute.

APPENDIX 1 – PERSONAL DATA SECURITY BREACH REPORT FORM

Please act promptly to report any data security breaches. If you discover a data security breach, please notify your Head of Department/Office immediately. Heads of Department/Office to complete Section 1 of this form and email it to the DP Officer/FOI Officer at foi@dkit.ie

Section 1: Notification of Data Security Breach	To be completed by Head of Dept/School/Office of person reporting incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number, DkIT address):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details	
Brief description of any action taken at the time of discovery:	
For Institute use	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by Lead Investigator in consultation with head of area affected by the breach and DP Officer/FOI Officer
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Institute or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements e.g. to research sponsors?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data ○ **Sensitive personal data** (as defined in the Data Protection Acts) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
○ Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas;	
○ Personal information relating to vulnerable adults and children;	
○ Detailed profiles of individuals including information about work performance, salaries	

or personal life that would cause significant damage or distress to that person if disclosed;	
○ Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
○ Security information that would compromise the safety of individuals if disclosed.	
Category of incident (1, 2a, 2b or 3):	
Reported to DP Officer/FOI Officer on:	
If level 2b or level 3, date escalated by Lead Investigator to the Institute's Emergency Management Team (EMT)	

Section 3: Action taken	**To be completed by DP Officer/FOI Officer**
Incident number	**e.g. DBH/2016/001**
Report received by:	
On (date):	
Action taken by responsible officer/s :	
Was incident reported to Gardaí?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to DP Officer/FOI Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of DP Officer/FOI Officer:	
Notification to Data Protection Commissioner	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**

APPENDIX 2 – CHECKLIST FOR ASSESSING SEVERITY OF THE INCIDENT

How serious is the incident?

Level 1: Local Incident:

- Is this a local incident?
  - Local incident = limited disruption to services (department, building or Institute); no serious threat to life, property or the environment; no threat to DkIT's image/reputation.
- Can the consequences of the security breach, loss or unavailability of the asset be managed locally within normal operating procedures?
- If so, manage the incident according to the Data Security Breach Management Procedure (this procedure).

Level 2.a: Minor Emergency Type A – Unlikely to Escalate into a Major Emergency:

- Is this a Minor Emergency (type A)?
  - Minor Emergency (type A) = Disruption to the functioning capacity of a key Institute building or a key service. Situation or incident (actual or potential) which poses a threat to life, property or environment, at a minor level but may escalate to Type B.
- Do containment and recovery require assistance from other members of staff within the Institute or specialist support teams outside the Institute?
- Does the breach require a notification to the Institute's senior managers?
- If so, the Lead Investigator (liaising with the DP Officer/FOI Officer) will decide who else needs to assist or be made aware of the breach e.g.
  - President
  - Vice President for Finance & Corporate Affairs
  - Vice President for Academic Affairs & Registrar
  - Vice President for Strategy, Communications & Development
  - Institute Librarian
  - Human Resource Manager
  - Estates Manager

And so on.

Level 2.b: Minor Emergency Type B or Level 3: Major Emergency

- Is this a major incident?
- Does containment and recovery, or the consequences of the loss or unavailability of the asset, require significant Institute resources beyond normal operating procedures?
- If so, inform the President's Secretary who will follow the Institute's Emergency Response Plan.

The incident level is defined by:

- Does the incident need to be reported immediately to the Gardaí?
- How important an information asset is to the Institute business process or function
- Whether the asset is a vital record. Is it unique – once lost, lost forever? Will its loss have adverse financial legal, liability or reputational consequences e.g. evidential records required to defend the Institute's interests?
- Is it business-critical? Do you rely on access to this particular information asset or you can turn to reliable electronic copies or alternative manual processes e.g. paper files if the information asset is unavailable
- How urgently access would need to be restored to an information asset to resume business or, if a workaround will keep business moving in the short term, to return to the required standard of service
- Does the loss or breach of data security involve high risk personal data, i.e.:

    - **Sensitive personal data** (as defined in the Data Protection Acts) relating to a living, identifiable individual's
        a) racial or ethnic origin;
        b) political opinions or religious or philosophical beliefs;
        c) membership of a trade union;
        d) physical or mental health or condition or sexual life;
        e) commission or alleged commission of any offence, or
        f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

    - Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas;

    - Personal information relating to vulnerable adults and children;

    - Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;

    - Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.

    - Security information that would compromise the safety of individuals if disclosed.