University College Cork

Personal Data Security Breach Management Procedures

Version 1.2

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 University. These procedures supplement the University's Data Protection Policy which affirms the University's commitment to protect the privacy rights of individuals in accordance with Data Protection legislation.

TABLE OF CONTENTS

1. INTRODUCTION

University College Cork is obliged under the Data Protection Acts, 1988 to 2018 and the EU General Data Protection Regulation (GDPR) to keep personal data safe and secure and to respond promptly and appropriately to personal data security breaches. It is vital to take prompt action in the event of any actual, potential or suspected breaches of personal data security or confidentiality to avoid the risk of harm to individuals, damage to operational business and potential financial, legal and reputational costs to the University.

2. PURPOSE

The purpose of these procedures is to provide a framework for reporting and managing data security breaches affecting personal or special category data[1] held by the University. These procedures supplement the University'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 incident which gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data held by the University 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 University'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 University data, including:

[1] **Personal data** means information relating to an identified living individual or a living individual who can be identified from the data, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
Special categories of personal data (formerly known as "sensitive personal data") receive greater protection under the Data Protection Acts and refer to the following: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data or biometric data for the purpose of uniquely identifying a person; data concerning health; data concerning a person's sex life or sexual orientation. Data subjects have additional rights under Article 9 of the GDPR in relation to the processing of any such data. Whilst criminal convictions and offences are not classed as special categories of personal data, the Data Protection Acts also provide additional rights to data subjects in this regard.

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

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 University 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 University IT systems managed centrally by IT Services, and locally by individual Colleges/Schools/Departments/Offices/Institutes or Centres;
- any other IT systems on which University data is held or processed.

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

Personal data security breaches are managed by the Information Compliance Manager (Office of Corporate & Legal Affairs) in conjunction with the Corporate Secretary and the Director of IT Services (where appropriate), with ultimate responsibility resting with the Corporate Secretary.

In emergency situations, the University's **Emergency Management 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 University 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 Information Compliance Manager:**
  - **During office hours, phone extension 3949 (or 3411 if unavailable).**
  - **Outside of Office Hours, phone the University Emergency Number +353 (21) 4903111**
- **complete the attached Data Security Breach Report Form and email it to foi@ucc.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

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 University 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 **Information Compliance Manager**, Office of Corporate & Legal Affairs (phone 021 4903949 or email foi@ucc.ie). The line manager/head of department should complete part 1 of the Data Security Breach Report Form and return it to the Information Compliance Manager without delay. Part 1 of the Report Form will assist the Information Compliance Manager 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 Information Compliance Manager will, in consultation with the Corporate Secretary, decide if it is necessary to appoint a group of relevant University stakeholders to assist with the investigation. Any records relating directly to an investigation will be retained by the Information Compliance Manager.

The Information Compliance Manager and the Head of the area affected by the breach (with the Corporate Secretary where required), 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** (i.e. they will decide if the incident can be managed and controlled locally or if it is necessary to escalate the incident to the **University Emergency Management Team**). The severity of the incident will be categorised as level 1, 2a, 2b or 3.

The table below (extracted from the ***University's Emergency Response Plan***) outlines how incidents will be managed according to the severity of the incident.

Level	Emergency type	
1.	Local Incident	Managed and Controlled Locally
2.a	Minor Emergency Type (A)	
2.b	Minor Emergency Type (B)	Escalated to Emergency Management Team (EMT) which is responsible for the management & close-out of the incident
3.	Major Emergency	

Incidents deemed to be level 1 or level 2a will be managed locally using this procedure. Incidents deemed to be level 2b or level 3 will be escalated by the Corporate Secretary to the University's Emergency Management Team (EMT) who will take over responsibility 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 University needs to take immediate and appropriate action to limit the breach.

The Information Compliance Manager / Corporate Secretary and relevant University staff members/managers, will:

- Establish who within the University needs to be made aware of the breach (e.g. IT Services, Buildings & Estates, Legal (OCLA), Media and Public Relations 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 University 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 on Part 1 of the Data Security Breach Report Form will assist with this stage.

The Information Compliance Manager in conjunction with the head of department/unit/institute/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 University:
        - 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 Information Compliance Manager 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 Corporate Secretary and the Head of College/School/Department/Unit/Institute or Centre (as appropriate) affected by the breach. Heads of College/School/Department/Unit/Institute or Centre 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 University's Risk Management Policy and Emergency Plan.

Step 4: Notification

On the basis of the evaluation of risks and consequences, the Information Compliance Manager and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside the University. For example:

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

Notifying the Data Protection Commission:

Under GDPR, the University must report all data breaches to the Data Protection Commission, unless the breach "is unlikely to result in a risk to the rights and freedoms of data subjects" (s.86 of DPA 2018)**.**

Reporting of data breaches to the DPC must be made without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where the University does not notify the Commission within 72 hours, the University must include in the notification the reason for not doing so.

Any contact with the Commission should be made through the Information Compliance Manager or Corporate Secretary. Initial contact with the Commission should be made by the Information Compliance Manager within 72 hours of becoming aware of the breach, outlining the circumstances surrounding the incident. This initial contact should be by e-mail and must not involve the communication of personal data. The Commission 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 Information Compliance Manager and Corporate Secretary ***not*** to report a breach, a brief summary of the incident with an explanation of the basis for not informing the Data Protection Commission will be retained by the Information Compliance Manager.

Notifying the Data Subjects:

In certain cases, as well as notifying the Data Protection Commission, the University is also required to communicate a breach to the affected individuals. Article 34(1) of the GDPR states: *"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."* The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue. The GDPR states that communication of a breach to individuals should be made "*without undue delay,"* which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves. Depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.

As well as deciding **who** to notify, the Information Compliance Manager and Corporate Secretary must consider the following:

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

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

  - a description of the nature of the breach;
  - a description of the likely consequences of the breach;
  - how and when the breach occurred;
  - what data was involved;
  - a description of the measures taken or proposed to be taken by the University to address the breach;
  - the name and contact details of the Information Compliance Manager and other contact points.

When notifying individuals, the University should give specific and clear advice on what steps they can take to protect themselves from possible consequences of the breach (such as re-setting passwords), what the University is willing to do to assist them and should provide details of how they can contact the University 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.

NOTE: It is advisable that the Media and Public Relations Office are consulted prior to any notification to data subjects being made.

Step 5: Evaluation and Response

Subsequent to a data security breach, a review of the incident by the Information Compliance Manager in consultation with the relevant stakeholders in the University will take place to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

For each **serious** incident, the Information Compliance Manager and Corporate Secretary will conduct a review to consider 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?

The Information Compliance Manager will compile a central record of all personal data breaches and will report on incidents to the Corporate Secretary 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.

9. RELATED POLICIES AND PROCEDURES

These procedures underpin the following University policies and procedures:

- Data Protection Policy (https://www.ucc.ie/en/ocla/comp/data/dataprotection/)
- Acceptable Use Policy (https://www.ucc.ie/en/it-policies/policies/au-pol/)
- IT Security Policy (https://www.ucc.ie/en/it-policies/policies/security/)
- Records Management Policy (https://www.ucc.ie/en/ocla/univarch/records/rm-policy/)

UCC 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:

Catriona O'Sullivan
Information Compliance Manager
4 Carrigside, College Road
University College Cork
Cork

Phone: (021) 4903949
Email: foi@ucc.ie

11. DISCLAIMER

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

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 Information Compliance Manager at foi@ucc.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, UCC address):	
Brief description of incident or details of the information lost:	
Details of the IT systems, equipment, devices, records involved in the security breach:	
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 University use	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by Information Compliance Manager in consultation with head of area affected by the breach
Details of information loss:	
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 University or third parties?	
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 ○ **Special Categories of personal data** relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; d) membership of a trade union; e) genetic or biometric data; f) data concerning health; g) data concerning a person's sex life or sexual orientation; Also consider data relating to criminal convictions/offences as sensitive.	
○ 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):	
If level 2b or level 3, date escalated by Corporate Secretary to the University's Emergency Management Team (EMT)	

Section 3: Action taken	To be completed by Information Compliance Manager
If notified to Data Protection Commission, provide details, incl. date:	
If notified to data subjects, provide details, incl. date:	
If notified to other external, regulator/stakeholder, provide details:	
If reported to Gardai, provide details, incl. dates:	
If notified to other internal stakeholders, provide details and dates:	
Follow up action required/recommended:	

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 University); no serious threat to life, property or the environment; no threat to UCC'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 University 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 University or specialist support teams outside the University?
- Does the breach require a notification to the University's senior managers?
- If so, the Information Compliance Manager, liaising with the Corporate Secretary, will decide who else needs to assist or be made aware of the breach e.g.
  - President
  - Vice President for External Relations
  - Librarian/Head of Information Services
  - Corporate Secretary/Director of Human Resources
  - Registrar/Senior Vice President Academic
  - Vice President for External Relations
  - Vice President for Research Policy & Support
  - Bursar/Chief Financial Officer
  - Director of Buildings & Estates
  - Heads of College
  - Head of Internal Audit
  - Risk Manager

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 University resources beyond normal operating procedures?
- If so, inform the Corporate Secretary of the University who will follow the University'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 University 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 University'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.:

    - **Special Categories of personal data** (as defined in the Data Protection Acts) relating to a living, identifiable individual's
        a) racial or ethnic origin;
        b) political opinions
        c) religious or philosophical beliefs;
        d) membership of a trade union;
        e) data concerning health
        f) data concerning a person's sex life or sexual orientation.

        Also, consider as sensitive data relating to the commission or alleged commission of any offence/criminal convictions.

    - 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;

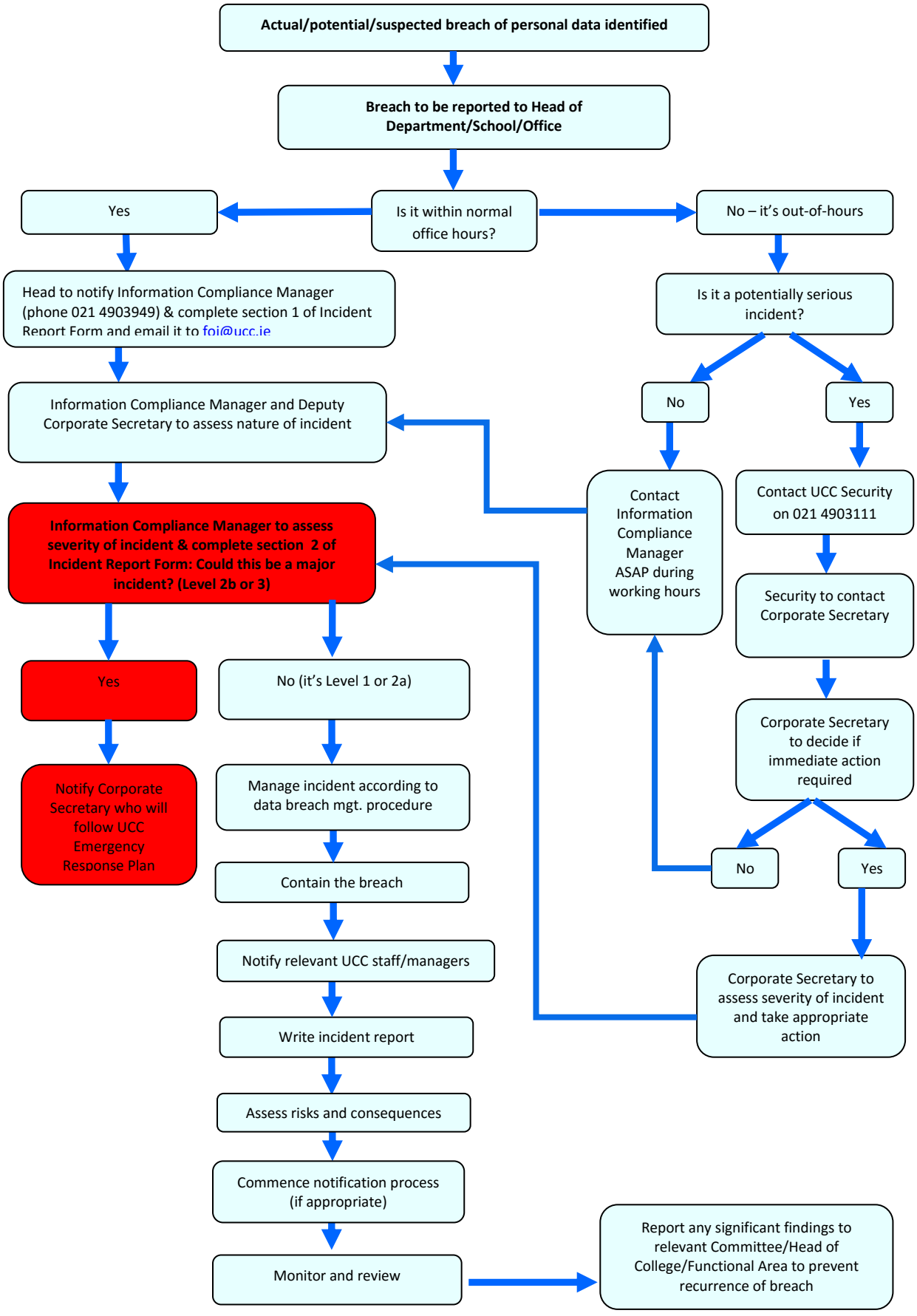
    - Personal information relating to vulnerable adults and children;

    - 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.

APPENDIX 3 –DATA SECURITY BREACH RESPONSE FLOWCHART



Document Location

>>>>>

Revision History

Date of this revision: 05/10/2018	Date of next review: 05/10/2019

Version Number/Revision Number	Revision Date	Summary of Changes
1.0	07/10/2013	Draft finalised
1.1	01/10/2018	Re-drafted in light of GDPR
2.0	05/10/18	Final version completed

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
0.1	20/11/12		1st draft of policy written
0.2	07/12/12	GC	2nd draft written (after comments by GC)
0.3	12/12/12		3rd draft written to simplify & streamline procedures
0.4	24/01/13	GC/NG/COS	Amendments made following meeting with GC/NG/COS
0.5	22/08/13	GC/NG/COS	Further amendments to simplify procedure
0.6	17/09/13	NG/COS	Further minor amendments throughout
0.7	19/09/13	GC	No changes required

Approval

This document requires the following approvals:

Title	Date
Corporate Secretary	05/10/18