**University College Cork**

**Personal Data Breach**

**Management Procedures**

**Version 3**

****

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](https://www.ucc.ie/en/ocla/comp/data/dataprotection/%20) which affirms the University’s commitment to protect the privacy rights of individuals in accordance with Data Protection legislation

TABLE OF CONTENTS

[1. INTRODUCTION 3](#_Toc178685552)

[2. PURPOSE 3](#_Toc178685553)

[3. What is a PERSONAL Data Breach? 3](#_Toc178685554)

[4. Who do these procedures apply to? 4](#_Toc178685555)

[5. What TYPES OF DATA do these procedures apply to? 4](#_Toc178685556)

[6. WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA BREACHES? 4](#_Toc178685557)

[7. PROCEDURE FOR *REPORTING* PERSONAL DATA BREACHES 5](#_Toc178685558)

[8. PROCEDURE FOR *MANAGING* PERSONAL DATA BREACHES 5](#_Toc178685559)

[Step 1: Identification and Initial Assessment of the Incident 5](#_Toc178685560)

[Step 2: Containment and Recovery 6](#_Toc178685561)

[Step 3: Risk Assessment 7](#_Toc178685562)

[Step 4: Notification 8](#_Toc178685563)

[Notifying the Data Protection Commission: 8](#_Toc178685564)

[Notifying the Data Subjects: 9](#_Toc178685565)

[Step 5: Evaluation and Response 10](#_Toc178685566)

[9. RELATED POLICIES AND PROCEDURES 10](#_Toc178685567)

[10. FURTHER HELP AND ADVICE 11](#_Toc178685568)

[11. DISCLAIMER 11](#_Toc178685569)

[APPENDIX 1 – PERSONAL DATA BREACH REPORT FORM 12](#_Toc178685570)

[**PERSONAL DATA BREACH REPORT FORM** 12](#_Toc178685571)

[APPENDIX 2 – CHECKLIST FOR ASSESSING SEVERITY OF THE INCIDENT 20](#_Toc178685572)

[APPENDIX 3 – PERSONAL DATA BREACH RESPONSE FLOWCHART 22](#_Toc178685573)

# 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 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.

# PURPOSE

The purpose of these procedures is to provide a framework for reporting and managing personal data breaches affecting personal or special category data[[1]](#footnote-1) held by the University. These procedures supplement the University’s [Data Protection Policy](https://www.ucc.ie/en/ocla/comp/data/dataprotection/%20), which affirms its commitment to protect the privacy rights of individuals in accordance with Data Protection legislation.

# What is a PERSONAL Data Breach?

A personal data breach is any incident that gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data held by the University in any format. Personal data breaches can happen for a number of reasons, including:

* Loss or destruction of personal data (accidental or deliberate)
* the disclosure of confidential data to unauthorised individuals
* loss or theft of data, device or equipment on which data is stored (encrypted or unencrypted)
* loss or theft of paper records
* unauthorised access to data/inappropriate access controls
* suspected breach of the University’s IT security and Acceptable Use policies
* attempts to gain unauthorised access to computer systems, e.g. hacking
* social engineering attack (e.g. phishing, vishing, smishing incident)
* records altered or deleted without authorisation by the data “owner”
* virus, ransomware, denial-of-service or other attack on IT systems or network
* 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
* email and/or attachments sent to incorrect recipient(s)
* email sent to mailing list without using BCC function
* Online publication (deliberate)
* Online publication (accidental)
* Processing error
* System maintenance - end of life, software development, system configuration
* Inappropriate disposal of equipment/assets
* Inappropriate disposal of paper

# Who do these procedures apply to?

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

* 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 or research activities
* individuals who are not directly employed by the University, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for the University
* people on placement, visiting students and researchers, volunteers
* members of UCC's Governing Authority in the course of their duties

Hereinafter collectively referred to as “**Members**”.

# What TYPES OF DATA do these procedures apply to?

These procedures apply to:

* all personal data created or received by the University, in the course of University business, in any format (including paper and electronic 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
* research data being created or stored in any format (including paper and electronic records) either on campus or at another site where UCC is a Data Controller or Joint Controller of the research data
* any other IT systems on which University data is held or processed and in respect of which the University is a Controller

# WHO IS RESPONSIBLE FOR MANAGING PERSONAL DATA BREACHES?

Personal data breaches are managed by the Information Compliance Manager (Office of Corporate & Legal Affairs) in conjunction with the Deputy Corporate Secretary and the IT Security Officer/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).

# PROCEDURE FOR *REPORTING* PERSONAL DATA BREACHES

**In the event of a personal data breach 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 personal data breach, he/she must report the incident to their Head of School/Unit immediately.**

**The Head of School/Unit must then:**

* **report the incident** **immediately to the Information Compliance Manager:** 
  + **By emailing** [**gdpr@ucc.ie**](mailto:gdpr@ucc.ie)
  + **During office hours, phone extension 3949 (or 3411 if unavailable)**
  + **Outside of office hours, phone the University Emergency Number +353 (21) 4903111**
* **complete part 1 of the attached Personal Data Breach Report Form and email it to** [**gdpr@ucc.ie**](mailto:gdpr@ucc.ie) **as soon as possible**

If the data breach involves clinical research data, the breach must also be reported immediately to the Clinical Research Reporting Officer (CRRO), copying gdpr@ucc.ie. A copy of the Personal Data Breach Report Form should be sent to the CRRO. This can be done by the Head of School by emailing PFRSponsor@ucc.ie.

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.

# PROCEDURE FOR *MANAGING* PERSONAL DATA BREACHES

The following 5 steps should be followed in responding to a personal data 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 personal data breach has occurred, this must be reported immediately to the member’s Head of School/Department/Line Manager who will in turn notify the Information Compliance Manager, Office of Corporate & Legal Affairs, by email at gdpr@ucc.ie. The Head of School will also notify the CRRO where the breach involves clinical research data by emailing PFRSponsor@ucc.ie.

The Head of Department/Line Manager should complete part 1 of the Personal Data 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 breach has taken place; if so:
* the personal data involved
* the cause of the breach
* the extent of the breach (how many individuals are affected)
* harm to affected individuals
* any measures that have been taken to mitigate 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/Deputy 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/Deputy 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)  Escalated to Emergency Management Team (EMT) which is responsible for the management & close-out of the incident |
| 2.b | Minor Emergency Type (B) |
| 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 personal data breach has occurred, the University needs to take immediate and appropriate action to limit the breach.

The Information Compliance Manager/Corporate Secretary/Deputy 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), Office of Media and Communications) and discuss what can be done 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.) and any communications that might be necessary
* 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 personal data 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 Personal Data Breach Report Form will assist with this stage.

The Information Compliance Manager, in conjunction with the Head of Department/Line Manager of the area 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 complete Sections 2 & 3 of Data Breach Report form, setting out (where applicable):

* a summary of the breach
* the people involved in the breach, (such as staff members, students, contractors, external clients)
* details of the information, IT systems, equipment or devices involved in the 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 breach
* unrealised, potential consequences of the breach
* possible courses of action to prevent a repetition of the 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/Deputy Corporate Secretary and the Head of Department/Line Manager (as appropriate) affected by the breach. The Head of Department/Line Manager 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
* if the breach involves clinical research data, the CRRO will need to consider if there has been a serious breach of Good Clinical Practice (GCP) which will need to be reported to the Health Products Regulatory Authority (HPRA) and National Research Ethics Committee (NREC) who have approved the study and /or other regulatory / supervisory authorities connected with the clinical research study

## Notifying the Data Protection Commission:

**Under GDPR, the University must report all personal 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”

**Reporting of 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, the Deputy Corporate Secretary or the 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 involves the completion of an online breach notification form and must not involve the communication of personal data. Subsequent information may be provided by way of update via a supplementary online form quoting the reference number given by the Commission in relation to the initial notification. 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/Deputy Corporate Secretary, ***not*** to report a breach, an explanation of the basis for not informing the Data Protection Commission will be recorded in Section 3 of the University Personal Data Breach Report form 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/ Deputy 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?

The University must consider what the most appropriate method of notification is (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 Office of Media and Communications are consulted prior to any notification to data subjects being made.**

# Step 5: Evaluation and Response

Subsequent to a personal data 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/Deputy 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/Deputy 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.

# 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://uccireland.sharepoint.com/sites/UCCITPolicies/SitePages/IT-Security-Policy.aspx
* Records Management Policy <https://www.ucc.ie/en/ocla/archives-and-records/records-management/policy/>

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

# 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*

Office of Corporate & Legal Affairs

University College Cork

4 Carrigside, College Road

Cork

Email: [gdpr@ucc.ie](mailto:gdpr@ucc.ie)

Phone: (021) 4903949

# 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 BREACH REPORT FORM

|  |  |
| --- | --- |
| **C:\Users\catrionamartin\Downloads\UCC Logo RGB_NEW.jpg  PERSONAL DATA BREACH REPORT FORM** | |
| * **Use this form to report any suspected or actual breach of personal data.** * **If you discover a data security breach involving personal data, notify your Head of School/Unit immediately.** * **Complete Section 1 of this form in conjunction with your Head of School/Unit and email it to** [**gdpr@ucc.ie**](mailto:gdpr@ucc.ie) **without delay.** * **PLEASE NOTE: The University must report data breaches to the Data Protection Commission within 72 hours of discovering the breach so prompt action is essential.** | |
| **SECTION 1:  NOTIFICATION OF DATA BREACH** | **TO BE COMPLETED BY HEAD OF SCHOOL/UNIT OR PERSON REPORTING INCIDENT** |
| **Name and job title of person reporting incident:** |  |
| **School/Unit:** |  |
| **Contact details of person reporting incident (email address, telephone number):** |  |
| **Head of School/Unit (if different from above):**  ***NOTE: Please ensure that your Head of School/Unit is fully informed of this incident*** |  |
| **When did the breach initially occur?** | Date: Click or tap to enter a date.  Time:  Is this an estimated time? Yes  No |
| **Is the breach ongoing?** | Yes  No  If you selected “No”, when did the breach end? Click or tap to enter a date.  Comments: |
| **Have you secured/retrieved/restored the breached data?** | Yes ☐ No ☐ |
| **If data was lost, do you have a backup copy?** | Yes ☐ No ☐ Not applicable ☐ |
| **When did you become aware of the breach?** | Date: Click or tap to enter a date.  Time: |
| **If you became aware of the breach more than 72 hours ago, please give reasons for the delay in reporting the incident:** |  |
| **How were you made aware of the breach? (e.g. notified by an affected individual, staff member realised that the breach had occurred, etc.)** |  |
| **Does the breach involve a data processor/s? (i.e. a third party acting on behalf of UCC)** | Yes  No  If you selected “Yes”, please insert name/s and address/es of data processor/s: |
| **What is the nature of this breach? Please tick all applicable box(es):** | loss of device/equipment (encrypted)  loss of device/equipment (unencrypted)  theft of device/equipment (encrypted)  theft of device/equipment (encrypted)  Loss or destruction of personal data (accidental)  Loss or destruction of personal data (deliberate)  loss of paper records  theft of paper records  breach of physical security (e.g. break-in to room or cabinet containing personal data)  hacking incident  social engineering attack (e.g. phishing, vishing, smishing incident)  virus, ransomware, denial-of-service or other attack on IT systems or network  unauthorised access to data/inappropriate access controls  email and/or attachments sent to incorrect recipient(s)  email sent to mailing list without using BCC function  Processing error  System maintenance - end of life, software development, system configuration  Inappropriate disposal of equipment/assets  Inappropriate disposal of paper  other – not listed above, please elaborate below: |
| **Description of incident (please provide full details of what happened):** |  |
| **What was the cause of the breach? i.e. How did the incident occur? (e.g. employee error or omission, intentional unauthorised access)** |  |
| **How many individuals (data subjects) are affected, if known?** |  |
| **How many records were affected, if known?** |  |
| **What identifying details relating to individuals were disclosed (e.g. names, dates of birth, contact details, PPS numbers, exam results, etc.)?** |  |
| **Were any of the following special categories of personal data disclosed?** | racial or ethnic origin  political opinions  religious or philosophical beliefs  trade union membership  data concerning health  data concerning a person’s sex life or sexual orientation  genetic data  biometric data  other – not listed above, please elaborate here:  No special categories of personal data were disclosed |
| **Were vulnerable individuals affected (e.g. patients, children, people with disabilities)?** | Yes  No  If yes, please provide details: |
| **Were any details relating to criminal convictions or offences disclosed?** | Yes  No  If yes, please provide details: |
| **Is the data bound by any contractual security arrangements e.g. to research sponsors?** | Yes  No  If yes, please provide details: |
| **Does the breach involve cross-border processing of personal data? Are individuals (data subjects) in another country likely to be affected?** | Yes  No  If yes please provide details: |
| **Describe the action(s) taken to respond to the breach at the time it was discovered:** |  |
| **What technical or organisational measures were in place before the breach to prevent such an incident (e.g. staff training, access controls, encrypted laptop/device, other technical measures, etc.)?** |  |
| **What deficiencies in these technical or organisational measures have you identified as a result of this breach?** |  |
| **In your view, what are the potential consequences for the individual(s) as a result of this data breach? (e.g. loss of privacy, reputational damage)** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **For University use:** | | | |
| **Report received by Information Compliance Manager on (date & time):** |  | | |
| **Reference Number:** | **DSB/year/000 | ABCDXXX.XX** | | |
| **SECTION 2:  RISK ASSESSMENT** | **TO BE COMPLETED BY INFORMATION COMPLIANCE MANAGER IN CONSULTATION WITH HEAD OF SCHOOL/UNIT** | | |
| **SCALE OF DATA BREACH:** |  |  | |
| **Assessment of SCALE of data lost/disclosed:**  (based on how much data has been lost/disclosed, how many people were affected, how many records were lost/disclosed)? | Risk Assessment:  1. VERY LOW  2. LOW  3. MEDIUM  4. HIGH  5. VERY HIGH | Reason for score: | |
| **SENSITIVITY OF DATA BREACH:** |  |  | |
| **Please provide details of any types of information that fall into any of the following high risk categories:** |  | | |
| **Special category data** (as defined in GDPR) relating to living, identifiable individuals: | racial or ethnic origin  political opinions  religious or philosophical beliefs  trade union membership  data concerning health  data concerning a person’s sex life or sexual orientation  genetic data  biometric data  other   If you have ticked any of the above, please provide details of the type of data below: | | |
| Data relating to criminal offences or convictions | Yes  No  If yes, please provide details: | | |
| 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; | Yes  No  If yes please provide details: | | |
| Personal information relating to vulnerable adults and children; | Yes  No  If yes please provide details: | | |
| 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; | Yes  No  If yes please provide details: | | |
| Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals. | Yes  No  If yes, please provide details: | | |
| Security information that would compromise the safety of individuals if disclosed. | Yes  No  If yes, please provide details: | | |
| **Assessment of SENSITIVITY of data lost/disclosed:** | Risk Assessment:  1. VERY LOW  2. LOW  3. MEDIUM  4. HIGH  5. VERY HIGH | Reason for score: | |
| **CONSEQUENCES OF DATA BREACH:** |  | | |
| **Could the breach have adverse consequences for the affected individuals? Will it adversely affect their rights and freedoms?** | Yes  No  If yes, please explain: | | |
| **Is the data bound by any contractual security arrangements e.g. to research sponsors?** | Yes  No  If yes, please give details: | | |
| **Assessment of CONSEQUENCES of data lost/disclosed:** | Risk Assessment:  1. VERY LOW  2. LOW  3. MEDIUM  4. HIGH  5. VERY HIGH | Reason for score: | |
| **OVERALL RISK ASSESSMENT:** | Risk Assessment:  1. VERY LOW  2. LOW  3. MEDIUM  4. HIGH  5. VERY HIGH | Reason for score: | |
| **Category of incident (1, 2a, 2b or 3):**  **(as defined in UCC’s** [**Emergency Management & Business Continuity Plan**](https://uccireland.sharepoint.com/sites/OCLAPolicies/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FOCLAPolicies%2FShared%20Documents%2FEmergency%20Planning%20and%20Business%20Continuity%20Management%2FEmergency%20Management%20and%20Business%20Continuity%20Plan%20%2D%20FINAL%20%2D%20June%202021%2Epdf&parent=%2Fsites%2FOCLAPolicies%2FShared%20Documents%2FEmergency%20Planning%20and%20Business%20Continuity%20Management)**)** | 1  2a  2b  3 | | |
| **If level 2b or level 3, date escalated to the University’s Emergency Management Team (EMT)?** |  | | |
| **SECTION 3:  ACTION TAKEN / NOTIFICATION** | **TO BE COMPLETED BY INFORMATION COMPLIANCE MANAGER** | |
| Please **provide details of any measures you have put in place** in order to mitigate the impact of this personal data breach on the rights and freedoms of affected data subjects |  | |
| Please provide **details of any measures which will be put in place** in order to mitigate the impact of this personal data breach on the rights and freedoms of affected data subjects, and the expected implementation date |  | |
| Please provide **details of any** **technical or organisational measures** **which you have put in place following this breach** in order to ensure the appropriate security of personal data against such a personal data breach reoccurring |  | |
| **Was incident reported to other *internal* stakeholders (provide details and dates)?** | Yes  No  If yes, please elaborate here: | |
| **Is notification to the Data Protection Commission required?** | Yes  No  Provide reasons for decision below: | |
| **Has the Data Protection Commission been notified of this incident?** | Yes  No  If ‘Yes’, specify date: Click or tap to enter a date. | |
| **Is notification to the affected data subjects required?** | Yes  No  Provide reasons for decision below: | |
| **Have affected data subjects been informed?** | Yes  No  If ‘Yes’, specify date: Click or tap to enter a date.  How were they informed (e.g. by email, post, newspaper): | |
| **Was incident reported to Gardaí?** | Yes  No  If yes, please specify date reported:  Reason for decision to report to Gardaí: | |
| **Was incident reported to other external regulators/stakeholders?** | Yes  No  If ‘Yes’, please specify and provide reason for decision: | |

# 

# 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 (school, 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 breach, loss or unavailability of the asset be managed locally within normal operating procedures?
* If so, manage the incident according to the Personal Data 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/Deputy 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
* Chief People and Culture Officer
* Deputy President and Registrar
* Vice President for Global Engagement
* Vice President for Research Policy & Support
* Vice President for Learning and Teaching
* 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 can you 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 personal data 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

1. racial or ethnic origin
2. political opinions
3. religious or philosophical beliefs
4. membership of a trade union
5. data concerning health
6. 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 – PERSONAL DATA BREACH RESPONSE FLOWCHART

**Actual/potential/suspected breach of personal data identified**

No – it’s out-of-hours

Is it within normal office hours?

No (it’s Level 1 or 2a)

Notify Corporate Secretary who will follow UCC Emergency Response Plan

**Information Compliance Manager to assess severity of incident & complete section 2 of Incident Report Form: Could this be a major incident? (Level 2b or 3)**

Yes

Monitor and review

Assess risks and consequences

Is it a potentially serious incident?

Yes

**Breach to be reported to Head of Department/School/Office**

Yes

Head to notify Information Compliance Manager (phone 021 4903949) & complete section 1 of Incident Report Form and email it to [gdpr@ucc.ie](mailto:gdpr@ucc.ie)

Information Compliance Manager and Deputy Corporate Secretary to assess nature of incident

Complete UCC Personal Data Breach Report from

Commence notification process (if appropriate)

Security to contact Corporate Secretary

No

Contact Information Compliance Manager ASAP during working hours

Contact UCC Security on 021 4903111

Corporate Secretary to decide if immediate action required

Contain the breach

Manage incident according to data breach mgt. procedure

Notify relevant UCC staff/managers

Report any significant findings to relevant Committee/Head of College/Functional Area to prevent recurrence of breach

No

Yes

Corporate Secretary to assess severity of incident and take appropriate action

**Document Location**<https://www.ucc.ie/en/ocla/legal-infocomp/informationcompliance/dataprotectiongeneral/>  
  
**Revision History**

|  |  |
| --- | --- |
| **Date of this revision:** 15/10/2024 | **Date of next review:** October 2026 |

|  |  |  |
| --- | --- | --- |
| **Version Number/Revision Number** | **Revision Date** | **Summary of Changes** |
| 1.0 | 07/10/2013 | Draft finalised (having regard to Guidance for Public Sector Bodies) |
| 2.0 | 05/10/2018 | Final version completed (having regard to GDPR) |
| 3.0 | 15/10/2024 | Final review completed |

**Consultation History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Number** | **Consultation Date** | **Names of Parties in Consultation** | **Summary of Changes** |
| 0.1 | 20/11/2012 |  | 1st draft of policy written |
| 0.2 | 07/12/2012 | GC | 2nd draft written (after comments by GC) |
| 0.3 | 12/12/2012 |  | 3rd draft written to simplify & streamline procedures |
| 0.4 | 24/01/2013 | GC/NG/COS | Amendments made following meeting with GC/NG/COS |
| 0.5 | 22/08/2013 | GC/NG/COS | Further amendments to simplify procedure |
| 0.6 | 17/09/2013 | NG/COS | Further minor amendments throughout |
| 0.7 | 19/09/2013 | GC | No changes required |
| 1.1 | 01/10/2018 | GC/NG/COS | Re-drafted in light of GDPR |
| 2.1 | 01/08/2024 | NG/AH/CS/DC/GC/BF/ | Review & updated of procedures commenced |
| 2.2 | 01/10/2024 | DO’C/EH/PC/NP/SC/SRM/AW | Consulted IT Services, Teaching and Learning, People and Culture, OVPRI, Media & Communications, UCC Security, Enterprise Risk Management and College/School Heads & Managers involved in recent breaches. |
| 3.0 | 15/10/2024 | PMcS/TE/MD | Amendments suggested and made following consultation |

**Approval**

This document has been approved as follows:

|  |  |
| --- | --- |
| **Title** | **Date** |
| Corporate Secretary | 23/10/2024 |
| University Leadership Team (ULT) | 23/10/2024 |

1. **Personal data**means information relating to an identified living individual or a living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person can identify an individual or make them identifiable.

   **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. [↑](#footnote-ref-1)