|  |  |
| --- | --- |
| 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 of person reporting incident:** |  |
| **School/Unit:** |  |
| **Contact details of person reporting incident (email address, telephone number):** |  |
| **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. |
| **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.)** |  |
| **What is the nature of this breach? Please tick all applicable box(es):** | loss or theft of device/equipment  loss or 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  other – not listed above, please elaborate below: |
| **Description of incident (please provide full details of what happened):** |  |
| **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 below: |
| **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 |
| **Have you secured the breached data?** | Yes  No  Please provide details: |
| **If data was lost, do you have a backup copy?** | Yes  No  Not applicable |
| **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?** |  |
| **For University use:** | |
| **Report received by Information Compliance Manager on (date & time):** |  |
| **Reference Number:** | **DSB/year/000 | INFC20XX.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: | |
| **Could the breach have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?** | 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 by Lead Investigator to the University’s Emergency Management Team (EMT)?** |  | |

|  |  |
| --- | --- |
| **SECTION 3:  ACTION TAKEN / NOTIFICATION** | **TO BE COMPLETED BY INFORMATION COMPLIANCE MANAGER** |
| **Follow up action(s) required/recommended:** |  |
| **Have these actions been carried out?** | Yes  No  If not, when are they expected to be completed? Click or tap to enter a date. |
| **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: |