**Personal Data Breach/Incident Report Form**

For more details please see the University’s Personal Data Breach Procedure which relates to this form. [Breach / Incident Reporting (napier.ac.uk)](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/Breach-and-Incident-Reporting.aspx)

|  |  |
| --- | --- |
| **Breach reference number** | IGxxx-xx |
| **Status of breach** | Choose a status  |

|  |
| --- |
| **Contact details of person reporting personal data breach/incident** |
| **Name:** |  |
| **Job title:** |  |
| **School/Department:** |  |

|  |
| --- |
| **Information about the personal data breach/incident** |
| **Date/time incident notified:** | **Date** |  | **Time** |  |
| **Date/time incident discovered:** | **Date** |  | **Time** |  |
| **Date incident occurred:** please note time periods if data was exposed for a prolonged period rather than a single incident (if known) |  |
| **What was the duration of the incident?** e.g. how long was the data disclosed for? |  |
| **Full description of incident/ breach:** |  |
| **What was the nature of the activity/processing being undertaken at the time the incident occurred?** |  |
| **Format of breach:**  |
|[ ]  Email | [ ]  | Other: |
|[ ]  Website |  |  |
|[ ]  Hardcopy/paper document loss |  |  |
|[ ]  Shared drive |  |  |
|[ ]  Mobile device |  |  |
|[x]  Miss-use of login details |  |  |
| **How was the incident discovered:** |  |
| **Who was the incident/breach reported to:** |  |
| **Have you informed your line manager?** (They will be contacted as part of the Governance follow up) |  |
| **Primary cause of breach** |
|[ ]  Malicious attack/cyber incident |[ ]  Other: |
|[ ]  Accident (e.g. system failure) |  |  |
|[ ]  Negligence (e.g. human error) |  |  |
| **Origin of breach** |
|[ ]  Internal (e.g. staff or student) |[ ]  External – third party controller |
|[ ]  External – third party processor |[ ]  External – other third party |
| **Details of information disclosed:** |
| **Personal data fields:** e.g. name, home address, term-time address, mobile number, phone number, private email address, exam/assessment marks, achievement or employment information (CV), financial information, location data, IP address, etc. |  |
| **Sensitive personal data:** e.g. health information, racial or ethnic origin, sexual orientation or sex life, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data. |  |
| **Confidential information:** e.g. draft business plans, unapproved strategy documents, financial information, information exempt under FOI/EIRs, information provided in confidence, pre-tender documentation, etc. |  |
| **What is the** [**information classification**](http://staff.napier.ac.uk/services/secretary/governance/records/Documents/Information%20Security%20Classification%20Scheme%20V2.0.pdf)**:** e.g. red, amber, yellow, green |  |
| **Please cut and paste evidence/text or provide as attachment if possible e.g. forward copy original email with any attachments showing all recipients.****This may be necessary for immediate action to mitigate the impact of the incident so please provide in full.** |
| **Further information concerning the personal data breach** |
|  |

|  |
| --- |
| **Assessment of the personal data breach/incident** |
| **How many individuals were affected:** (had their personal data disclosed)(approximate number if exact not known) |  |
| **How many individuals received or had access to the personal data:**Please detail how many were external and how many were internal to the University. |  |
| **Does the incident/breach involve data shared with, or received from, other 3rd party organisations / educational institutions?** e.g. where we are bound by contract to inform them of a breach |  |
| **What immediate remedial action was taken?** e.g. email recalled, document removed from website, security issue rectified |  |
| **Other action/s:** |  |

|  |  |
| --- | --- |
| **Categories of individuals affected** |[ ]  Prospective students |
|  |[ ]  Current students |
|  |[ ]  Alumni |
|  |[ ]  Staff (other than senior staff) |
|  |[ ]  Senior staff |
|  |[ ]  Research participants |
|  |[ ]  Other: |  |

|  |
| --- |
| **Likely impact of the breach** |
|[ ]  Breach of confidentiality |[ ]  Liability issues |
|[ ]  Business interruption |[ ]  Loss of personal data |
|[ ]  Damage to University’s reputation |[ ]  Property damage |
|[ ]  Damage to individuals’ reputation |[ ]  Re-identification of individuals |
|[ ]  Direct financial loss |[ ]  Reversal of pseudonymisation |
|[ ]  Discrimination |[ ]  Unauthorised access to systems |
|[ ]  Emotional distress |[ ]  Other:  |
|[ ]  Harassment or victimisation |  |  |
|[ ]  Identity theft or fraud |  |  |

|  |
| --- |
| **Existing security measures** |
| Were any risks identified in this activity/processing prior to the incident? | Yes/no |
| If yes, please provide detail: |  |
| How was this incident identified: e.g. through audit or privacy impact assessment, notification by recipient of information, etc. |  |
| What security measures were in place to protect the data: |  |
| When were risks/security measures last reviewed? Has a PIA/Audit been done? |  |
| **Other** |
| Has any data subject suffered any harm/damage due to this incident? If so please describe in full. |  |

**Information Services/Governance Services Use Only**

Main IG contact:

|  |
| --- |
| **Details of personal data breach/incident** |
| Action on notification of incident/ breach (incl. other remedial action): |  |
| What was the cause of the incident? |  |
| Were sufficient security measures/ risk mitigations in place at time of incident? |  |
| Has the line manager acknowledged that the incident indicates a risk and agreed to implement improvements to mitigate the risk? |  |
| Senior management notification: Yes/No/Who notified. |  |
| Was the incident warranted as likely to cause harm to individuals? Please provide details of justification for either decision. Risk rating table below will assist in making the decision. |  |
| Where the breach resulted in a high risk to the rights and freedoms of individuals were they notified? Please see guidance for notification below. |  |
| Was the incident rated as serious enough to warrant ICO notification within 72 hours? Please provide details of justification for either decision. Risk rating table below will assist in making the decision. |  |
| If the incident was reportable and not notified to the ICO within 72 hours what were the reasons? Reasons to accompany the notification. Can be provided in phases without undue delay. |  |
| Follow up remedial action (date and action): |  |
| Reported to Risk and Resilience Committee: |  |
| **Date incident closed:** |  |

|  |
| --- |
| **Review of personal data breach/incident** |
| **Root cause(s) of the breach** |
|  |
| **Lessons learned – preventing recurrence** |
|  |
| **Lessons learned – management of the breach** |
|  |
| **Recommendations for cascading lessons learned** |
|  |
| **Follow-up actions required in relation to the breach** |
|  |

|  |
| --- |
| **Personal Data Breach Management Timeline -****To record key events and actions taken** |
| **Date** | **Time** | **Action** | **Noted by** | **Approved by** | **Comments** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

The following risk rating for personal data categories provided by the ICO will assist with rating the risk:

|  |  |
| --- | --- |
| **Category of Personal Information** | **Initial risk score (indicative ICO score)** |
| Name | **Low** |
| Address & Contact details | **Low** |
| Age / DOB | **Low** |
| Gender | **High** |
| Biometric data  | **High** |
| CCTV, photos and other images (which are not biometric data) | **Moderate** |
| Race/ethnic origin | **High** |
| ID documentation, such as passport, national insurance number, ID card, driving licence details | **High** |
| Medical records | **High** |
| Medication records | **High** |
| Name and contact details of GP  | **Low** |
| Name and contact details of specialist medical professionals | **High** |
| Genetic data | **High** |
| Current marriage and partnerships | **Moderate** |
| Marital history | **Moderate** |
| Details of family and other household members | **Moderate** |
| Habits | **Low** |
| Housing | **Low** |
| Travel details | **Low** |
| Leisure activities | **Low** |
| Location Data | **High** |
| Membership of charitable or voluntary organisations | **Low** |
| Political opinions | **High** |
| Religious or philosophical beliefs | **High** |
| Trade Union membership | **High** |
| Sex life or sexual orientation | **High** |
| Free text about an individual, eg in emails, social media, livechat (must assume is SCD) | **High** (may vary depending on circumstances) |
| Employment and career history | **Low** |
| Recruitment | **Low** |
| Termination details | **High** |
| Attendance records | **Low** |
| Health and safety records | **High** |
| Performance appraisals | **Moderate** |
| Training records | **Low** |
| Security records | **Low** |
| Financial account / credit card details | **High** |
| Income | **Moderate** |
| Salary | **Moderate** |
| Assets and investments | **Moderate** |
| Payments | **Moderate** |
| Creditworthiness / Credit score | **Moderate** |
| Loans | **Moderate** |
| Benefits | **Moderate** |
| Grants | **Moderate** |
| Insurance details | **Moderate** |
| Pension details | **Moderate** |
| Goods or services supplied | **Low** |
| Marketing preferences | **Low** |
| Delivery preferences | **Low** |
| Licences issues | **Low** |
| Insurance details | **Low** |
| Records of unspent criminal convictions and offences | **High** |
| Records of spent criminal convictions and offences | **High** |
| Records of DBS checks | **High** |
| Criminal investigations records | **High** |

DP\_Incident\_Breach\_reporting\_form.docx

Version 3.1

Last updated: 03/08/23