EDINBURGH NAPIER UNIVERSITY

PROCEDURE FOR A BREACH OF PERSONAL DATA SECURITY

1. Introduction

1.1 **First action in the event of a breach:** For electronic data see section 6.1 and for manual data see section 6.2 . Please follow these steps immediately in the event of an incident or breach – any delay may significantly affect the University's ability to contain and rectify the security incident/breach. Please complete the appropriate fields on the report form at Appendix A after notifying the relevant colleagues as per section 6.

1.2 The University holds a large amount of data and information in both electronic and manual format. This may include personal or confidential information (about people), and also non-personal information which could be sensitive or commercial e.g. financial data.

1.3 All reasonable care must be taken therefore to protect the University's corporate information assets from incidents which could compromise their security, whether these occur accidentally or deliberately.

1.4 This procedure applies to a breach of personal data which has occurred through unauthorised or unintentional access and whether this data is held in electronic or manual format.

1.5 The General Data Protection Regulation (the Regulation) governs the University's obligations with regard to personal data and these include a requirement to keep personal data secure.

1.6 In the event of a breach occurring with personal data whatever format it is held in, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact and consequences of the breach and prevent a recurrence.

1.7 References in this procedure to the UK Information Commissioner (ICO) will apply also to a successor supervisory authority.

2. Purpose of the Procedure

2.1 The purpose of this procedure is to set out what should be done in response to a data breach or information security incident which may occur across the University to ensure that all appropriate actions are taken immediately to minimise the associated risks.

3. Scope

3.1 This procedure applies to all University employees, contractors, third party agents and any individual/s who have access to, or are handling personal data held by the University as a data controller or data processor.

4. Definition and types of a personal data breach or information security incident

4.1 A personal data breach or information security incident is an event which has caused, or has the potential to cause, damage to personal data held by the University as a data controller or data processor. The term ‘breach’ will apply to a data breach or an information security incident which has caused the loss of, or unauthorised access to, personal data as defined by the ICO.

4.2 Examples are:

- Accidental loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)
- Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- Unauthorised disclosure of sensitive or confidential information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the website without consent
- Compromised user account (e.g. accidental disclosure of user login details through phishing)
- Failed or successful attempts to gain unauthorised access to University information or information systems
- Equipment failure
- Malware infection
- Disruption to or denial of IT services
- Human error
- Blagging offences where information is obtained by deceiving the organisation holding it

5. The consequences of a breach

5.1 The ICO, who oversees the Regulation, has powers to impose civil monetary penalties up to a maximum of €20Million or 4% of annual global turnover for serious data breaches or to take other enforcement action.

5.2 The ICO also have powers to impose civil monetary penalties up to a maximum of €10Million or 2% of annual global turnover for less serious infringements, which include failure to report a breach of the Regulation.

5.2. A breach could not only damage the University’s reputation and its relationship with its stakeholders, but also expose the University, its staff or students to the risk of fraud or identity theft. In addition, considerable distress could be caused to the individuals concerned, as a result of which the University could be sued.

6. Procedure to be followed if a breach or information security incident occurs

6.1 Electronic Data breach

6.1.1 Where a breach of electronic data is detected and/or suspected the user, member of staff or person detecting the breach should report this immediately to the Information Security Manager and in their absence to the Information Services (IT)

Duty Manager. The Information Governance Manager (IG Manager) should be notified thereafter. Contact details available online here: http://staff.napier.ac.uk/services/cit/ContactUs/Pages/ContactUs.aspx and http://staff.napier.ac.uk/services/secretary/governance/Pages/who.aspx

6.1.2 If the breach occurs by email the member of staff must attempt to recall all affected emails immediately. Instructions are available on the staff intranet here: http://staff.napier.ac.uk/services/cit/StaffEmail/Pages/StaffEmail.aspx#FAQ9 . The original email should *not* be re-sent with a request for deletion – Governance Services will provide advice and template wording.

6.1.3 The Information Security Manager or in their absence the Information Services (IT) Duty Manager will immediately inform the Director, Information Services or other nominated person of the breach and initiate an investigation.

6.1.4 The Information Security Manager will also liaise with the IG Manager as soon as possible and in their absence, the Data Protection Officer (DPO).

6.1.5 The Information Security Manager will take all immediate, necessary and reasonable steps to protect the University's systems and data, including the removal of system access, data or software from the equipment.

6.1.6 The Information Security Manager will provide regular updates to the Director, Information Services or their nominee and the IG Manager as soon as possible and in their absence, the DPO, until the breach is contained or resolved.

6.1.7 The Information Security Manager will liaise with relevant Information Services staff to produce a report on the breach, the causes of it and the remedial actions taken and provide this to the Director, Information Services and the DPO.

6.2 Manual data breach

6.2.1 The user or member of staff who is responsible for and/or detects a breach of manual personal data must immediately inform their line manager and the Information Goverance Manager as soon as possible and in their absence, the DPO. Contact details are available on the staff intranet here: http://staff.napier.ac.uk/services/secretary/governance/Pages/who.aspx

6.2.2 The member of staff in consultation with or as directed by their line manager and/or the IG Manager or in their absence, the DPO, will take immediate steps to contain or mitigate the breach.

6.2.3 The line manager or their nominee will inform the Dean of School/ Director of Professional Service, or other senior member of staff in the area in which the breach has occurred and the IG Manager or in their absence, the DPO.

6.2.4 The line manager or their nominee will provide regular updates to the Dean of School/ Director of Professional Service or other senior member of staff in the area in which the breach has occurred and the IG Manager or in their absence, the DPO.

6.2.4 The Dean of School/Director of Professional Service or other senior member of staff, will consult with Governance Services, any other relevant staff and where applicable the University Secretary, to agree on the immediate actions to be taken to contain the breach.

7. Managing the consequences of the data breach or information security incident

7.1 The DPO and/or the IG Manager will decide in the particular circumstances of the breach whether it is serious enough to inform the University Secretary and will consult where appropriate with the Director, Information Services, the University's Information Security Officer or the Head, Campus Services.

7.2 The Dean of School, Director of Professional Service or the Information Security Manager as appropriate, or other senior members of staff in the area in which the breach has occurred, must establish as soon as reasonably possible:

- the exact nature of the breach
- the number of individuals who have been affected by the breach
- what steps need to be taken to contain the breach

The DPO and the IG Manager are then to be informed of the above and any other relevant information, as soon as reasonably possible.

7.3 The DPO will consult with the IG Manager and where appropriate the Director, Information Services and then refer to relevant guidance from the ICO (or successor supervisory authority). The DPO will then decide if any action is deemed necessary and if so, will seek the University Secretary's decision on whether to notify:

- the ICO
- the individuals who may have been affected.

7.4 Should the University Secretary deem it necessary to contact the individuals whose personal data has been affected, the area in which the breach has occurred will notify those individuals as soon as reasonably possible and advise the steps taken to mitigate the risks, to enable them to take such other measures as they may wish to protect themselves. Governance Services will provide a form of words for the area to amend to suit the circumstances.

7.5 If a large number of individuals are affected, the DPO will consult and agree with the University Secretary, Director of External Relations and Communications and where appropriate, the Director Information Services, about the posting of appropriate information on the University's intranet or student portal.

7.6 Where the ICO is to be notified of the breach, the DPO will in consultation with the IG Manager and the Director, Information Services as appropriate ensure that this is done timeously and in accordance with the ICO's procedure.

8. Actions to be taken after the breach or information security incident has been dealt with or resolved

8.1 The DPO will consult with the IG Manager and where appropriate, the University Secretary, the Director, Information Services and Director, Human Resources to consider whether the University's response to the breach was effective and/or if any action should be recommended to be taken with any member of staff, student or external user.

8.2 Where relevant, staff may be required to receive additional training and/or attend the next scheduled University Information Governance briefing on data protection and/or relevant Information Services training sessions in respect of the security and transfer of electronic data.

8.3 A report of a notifiable breach will be made to the next meeting of the University Information Governance Group, the Risk & Resilience Committee and to the University Court, if deemed necessary.

8.4 In the event that the ICO requires any action(s) to be taken, the DPO and where appropriate the Director, Information Services will be responsible for ensuring these are carried out and report accordingly to the University Secretary.

9. Preventing a recurrence

9.1 The Dean of School/ Director of Professional Service or other senior member of staff in the area in which the breach occurred will liaise with Governance Services and where relevant Information Services, to review process and procedures, to ensure that effective remedial measures have been taken to prevent a recurrence and monitor ongoing compliance.

10. Further information

- University's Data Protection Code of Practice: Security of Personal Data
- Information Services: Introduction to Information Security

11. Contact

Diana Watt
IG Manager
Room 5.B.18 Sighthill Campus
Edinburgh, EH11 4BN
☎: 0131 455 6257 🖱**:** D.Watt@napier.ac.uk

Graeme Hamilton
Information Security Manager
Room 3/51, Craiglockhart Campus
Edinburgh, EH14
☎: 0131-455-4551 🖱**:** G.Hamilton@napier.ac.uk

Edinburgh Napier University acknowledges the assistance of the University of Edinburgh, Robert Gordon University and the University of Greenwich in preparing this procedure.

Appendix A

Incident/Breach Report and Response Form

Details of incident:	
Full description of incident/ breach:	
What was the nature of the activity/processing being undertaken at the time the incident occurred?	
Format of breach: e.g. email, website, shared drive, mobile device, paper document lost/missing, miss-use of log-in details, etc.	
Date incident occurred: please note time periods if data was exposed for a prolonged period rather than a single incident (if known)	
Date incident discovered:	
How was the incident discovered:	
Who was the incident/breach reported to:	
Please cut and paste evidence/text or provide as attachment if possible e.g. forward copy original email with any attachments showing all recipients. Please provide in full, as this may be necessary for immediate action to mitigate the impact of the incident.	
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: e.g. red, amber, yellow, green	
Other:	
How many individuals' (data subjects) were affected (had their personal data disclosed)(approximate number if exact not known):	

What categories of data subjects were affected: e.g. students, staff, alumni, enquirers, prospective students, supporters, etc.	
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.	
What was the effect or likely consequences of the incident/breach on the data subjects affected?	
What was the duration of the incident? e.g. how long was the data disclosed for?	
Was this incident negligent in character? e.g. processing took place in contravention of policy, with existing security issues identified, against advice, etc.	
Action/s	
What immediate remedial action was taken: e.g. email recalled, document removed from website, security issue rectified	
Other action/s:	
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	
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?	
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. [1]	
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. [2]	
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:	