University of Dundee

Information Governance – Data Protection

Standard Operating Procedure – Data incidents

1. Scope

1.1 This procedure supports the members of the University during data incidents.

1.2 Data incidents are those issues that lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

1.3 The procedure provides a framework so that the circumstances, seriousness and potential impact of any incident can be established and necessary actions taken to

- recover data
- avoid escalation
- mitigate loss
- inform necessary personnel and regulatory agencies
- avoid recurrence

1.3 University staff are reminded that the best way to prevent data incidents is to practice good information security and at minimum to lock filing cabinets, desk drawers and office doors where personal or other sensitive information may be held and to encrypt and password protect memory sticks, computers, laptops or other portable electronic media. Where systems are known to contain personal or other sensitive data staff should seek advice from UoDIT on security measures and ensure that any advice is implemented fully.

1.4 WHEN IN DOUBT ABOUT THE MANAGEMENT AND TRANSFER OF PERSONAL OR OTHER SENSITIVE DATA STAFF SHOULD ALWAYS SEEK ADVICE FROM INFORMATION GOVERNANCE, LEGAL AND/OR UODIT.

2. Responsibilities

2.1 The Secretary of the University is responsible for the proper management of personal data in the University.

2.2 The Data Protection Officer has those responsibilities set out in the General Data Protection Regulation and supports institutional compliance accordingly.
2.3 The Library & Learning Centre and Culture & Information provide guidance and operational support on data protection matters.

2.4 Legal provide advice to the University as required/appropriate.

2.5 Directors and Deans are responsible for ensuring this procedure brought to the attention of their Schools or Service areas and for its implementation.

2.6 All staff are responsible for ensuring that any suspected loss is reported immediately and that University information is held securely and used appropriately at all times.

3. Procedure

3.1 Following the identification of an incident conduct a preliminary search to establish the circumstances.

3.2 Notify your Director/School Manager, the Data Protection Officer, the Director of LLC&CI and/or the Head of Information Governance immediately.

3.3 The following information is required:

   a. What information is involved (as far as can be establish from the preliminary search)?
   b. How much information is involved?
   c. What was the presumed location and time of the incident?
   d. How sensitive was that information? (For more information on judging sensitivity please see the University’s Information Security Classification at www.dundee.ac.uk/information-governance/dataprotection)
   e. In what format was the information held (paper, electronically, on a memory stick, on a laptop etc)?
   f. In what ways was the information secured?

3.4 The Head of Information Governance (or Director LLC&CI in their absence) will lead any investigation/process of immediate mitigation and require other sections of the University to take any and all immediate steps necessary to contain the incident as far as possible, mitigate its impact and minimise escalation.

3.5 During this process a group of key stakeholders including, but not limited to, the Secretary of the University, the Data Protection Officer, the Director of LLC&CI and the Director of Academic and Corporate Governance will convene remotely (usually by email) to make any decisions necessary concerning notification
to the Information Commissioner’s Office an/or data subjects. Such notification, if required, must be provided no later than 72 hours after the University becomes aware of an incident.

3.6 Advice will be sought from Legal as appropriate during any incident.

3.7 Where incidents are of sufficient seriousness the Head of Corporate Communications will be asked to implement their incident response plan alongside this procedure to ensure accurate information is provided to data subjects and other stakeholders.

3.8 The 72-hour notification period notwithstanding, recommendations may be provided to the Secretary of the University at the conclusion of any investigation. These may include:

a. Reporting of the breach to the police where criminal activity is suspected (eg where there is suspicion that data has been stolen).

b. Training for individuals or units on the proper handling of University information.

c. Disciplinary action where the actions of an individual or group are found to be *ultra vires* or negligent.

d. The dissemination of learning points to School Managers and Directors to minimise the potential for recurrence.

**Change control**

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial approval</td>
<td>23 April 2012</td>
<td>University Court</td>
</tr>
<tr>
<td>The Chief Technical Officer and the Director of Legal Services added as contacts when a potential breach is identified.</td>
<td>27 August 2013</td>
<td>Secretary of the University</td>
</tr>
<tr>
<td>New point added concerning immediate mitigation.</td>
<td>27 August 2013</td>
<td>Secretary of the University</td>
</tr>
<tr>
<td>Composition of group to consider breach updated to reflect changes in University structure.</td>
<td>27 August 2013</td>
<td>Secretary of the University</td>
</tr>
<tr>
<td>Contact names/numbers added to end of procedure.</td>
<td>27 August 2013</td>
<td>Secretary of the University</td>
</tr>
<tr>
<td>Procedure revised to reflect changes to University structure, learning from earlier incidents and new SOP</td>
<td>3 November 2015</td>
<td>Chief Information Officer, Secretary of the University</td>
</tr>
<tr>
<td>Template for information governance issues.</td>
<td>Revised in advance of GDPR.</td>
<td>April 2018</td>
</tr>
</tbody>
</table>