The University of Huddersfield

Personal Data Incident Procedure

1. Background

The University of Huddersfield is committed to a policy of protecting individuals' right to privacy in accordance with the General Data Protection Regulation 2016 (the GDPR), the Data Protection Act 2018 (the DPA) and the University's Data Protection Policy.

The University is required to take appropriate measures against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The GDPR requires the University to report certain types of personal data incidents to the Information Commissioner's Office within 72 hours of becoming aware of the incident and to maintain a log of all such incidents. It is therefore crucial that the University has a robust incident detection, investigation and internal reporting procedure in place so that we can ensure compliance with data protection legislation.

A data security incident can happen for a number of reasons. In general terms, it occurs whenever any personal data is lost, destroyed, corrupted or disclosed. Examples include:

- Loss or theft of data or equipment on which data is stored (e.g. loss or theft of a computer or portable device, such as a laptop, data stick or paper files)
- Unauthorised access to, deletion, use, or alteration of, personal data
- Loss of availability of personal data for example as a result of a computer malware attack
- Human error (e.g. sending data to the wrong recipient or accidentally deleting it)
- 'Blagging' offences where information is obtained by a third party through deception

2. Responding to a Data Protection Incident

When a data protection incident occurs at the University. The University must:

- **Assess** the nature and extent of the incident to determine whether it is a minor, moderate or high risk incident reportable to the ICO;
- **Mitigate** the effects of the incident as far as possible, for example by retrieving or replacing the data, or helping data subjects ensure they are not adversely affected by the incident
- **Prevent** future similar incidents, by reviewing the incident to see if there are any measures it could take that could prevent another similar incident in the future

The Data Protection Team are responsible for co-ordinating the response to a data protection incident. They will undertake the initial assessment and provide advice on appropriate mitigation and prevention measures. However, every member of the University community has an obligation to comply with the Data Protection Policy and Data Protection Law and are responsible for mitigating and preventing data incidents within their area.

3. Reporting an Incident

Should you discover an incident (even if you are not responsible for it), it is extremely important to ensure that it is dealt with immediately and appropriately to minimise the impact of the incident and to help prevent any recurrence. **You should report a breach as soon as it comes to your attention, even if you discover it outside of working hours**.

Members of the University should report any incident or suspected incident to their School or Service's Data Protection Champion and to the University's Data Protection Officer (DPO) immediately upon becoming aware of it via the Online Incident Reporting Form.

Data Protection Officer's contact details: email: data.protection@hud.ac.uk; tel: 01484 473 000. If, for any reason, the online reporting form is not available, then an email should be sent to the Data Protection Officer, and an online form completed as soon as reasonably practicable afterwards.

The Data Protection Team will co-ordinate the response to the incident. In their absence an incident report will be dealt with by an appropriate member of the University Secretary's Office.

Set out below is a guide to the procedure that the Data Protection Team will follow when they are made aware of a personal data incident.

4. Initial Assessment

The person reporting the incident should complete the Data Protection Incident Evaluation Form. Following receipt of a report of a suspected incident the DPO will consider whether an incident has occurred and assess the risks associated with it. The Data Protection Team may request additional information in order to complete an initial assessment on the severity of the incident. The Data Protection Champion for the relevant School/Service may be required to assist with this process.

The DPO will make an initial assessment of the severity of the incident and the Data Protection Team shall advise the reporter accordingly. Whilst the incident is being managed, the DPO shall keep this assessment under review, and shall advise if they consider that the risk assessment of the incident changes.

4.1 Minor to Moderate Incidents

Where the DPO considers that the incident is minor, or moderate and falls below the ICO reporting threshold, the Data Protection Team will liaise directly with the relevant staff members and (if appropriate) the relevant Data Protection champions to advise on such measures as need to be taken to mitigate the incident and prevent recurrence.

The Data Protection Team will notify the relevant Dean or Director that there has been an incident in their area and provide them with:

- A description of the incident
- Confirmation of the measures required for management and mitigation of the incident and to prevent any recurrence of such incidents
- Any additional relevant facts, for example if it is a repeat incident, or if there have been any issues in securing the appropriate information or actions.

Deans and Directors have overall responsibility for Data Protection within their area, and are therefore responsible for ensuring that incidents within their area are appropriately managed and all mitigation steps are completed.

The DPO (or their nominee) shall be responsible for completing a report documenting the reasons for their assessment and for ensuring that the Data Incident log is kept up to date.

4.2 Major Incident

Where the DPO considers that a reported incident is, or has the potential to be, a major incident which may require notification to the ICO, the following procedure shall be followed:

Immediately upon assessment, the DPO shall identify key individuals to include within an incident response working group, which may include:

- Deputy Vice-Chancellor
- The University Secretary
- The relevant Dean/Director
- Director of Marketing
- (where the incident involves the integrity of the University's IT systems) Information Security Manager
- (if appropriate) wellbeing and support services (for example, Student Services, Registry, Occupational Health or HR)
- (if appropriate) the incident reporter

The DPO shall notify the individuals that a major data incident has occurred and that they may be required to assist in managing the incident. If appropriate the DPO shall seek to arrange a round-table meeting with the members of the response group to discuss the incident as soon as practicable after it has been reported.

The DPO shall be responsible for co-ordinating the University's response to a major data incident and, in particular, they shall:

- Request any further information necessary to assess the incident
- Provide advice on immediate steps for incident mitigation
- Where appropriate, within 72 hours of the incident being identified complete an initial ICO notification report

Key personnel in the relevant working group shall prioritise responding to the incident and shall provide regular (daily) updates to the DPO on the progress they have made in collating information, responding to the incident and any suggestions they may have on further actions which can be taken to fully assess and mitigate the incident.

Upon completion of the investigation, the DPO will, if necessary, be responsible for sending a follow up report to the ICO providing a complete summary of the incident. The DPO shall be the key point of contact for communication with the ICO.

The DPO shall complete a report documenting their reasons for the assessment and ensure that a record of the incident is included within the University's Data Incident log. Upon completion of the investigation, the DPO shall prepare for Audit Committee and SLT a report summarising the incident and any action learning points identified during the investigation process.

5. Mitigation

When the University's data is subject to a data incident, it is important to ensure that any risks are fully mitigated. This means that, as far as possible, the data should be recovered, restored or protected, and that data subjects should be protected from any consequences of the incident.

Possible recommendations for mitigation may include, requiring staff to contact an erroneous recipient and requesting them to delete and/or destroy all copies of the data; or contacting the data subjects so that they can put alerts on their credit cards; or changing passwords or other security settings.

The more quickly appropriate mitigation measures can be put in place, the less likely it is that serious consequences will arise from an incident. However, if there is any in any doubt over what actions a department should take to mitigate an incident, they should speak to the Data Protection Team before taking any action.

6. Preventing a repetition of an incident

After completing the procedures set out above, the DPO will evaluate the incident and the effectiveness of the University's response to it.

The DPO will consider any changes that may be required to be made to University policies and procedures to prevent an incident from recurring and will publicise internally any learning outcomes from their investigation of an incident, including via Information Governance Group, Data Protection Champions and SLT, as appropriate. Major incidents will also be reported to Audit Committee.

Where a learning outcome has been identified, all relevant members of staff have a duty to ensure that any recommendations are fully considered and, if possible, actioned.