The University of Huddersfield

Personal Data Security Breach 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 1998 and its proposed replacement 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 breaches to the Information Commissioner's Office within 72 hours of becoming aware of the breach and to maintain a log of all breaches. Failure to comply with the GDPR can lead to enforcement actions, including fines of up to €20 million or, if higher, 4% of an organisation's annual turnover.

It is therefore crucial that the University has a robust breach detection, investigation and internal reporting procedure in place so that we can ensure compliance with data protection legislation.

2. What is a data security breach?

A data security breach can happen for a number of reasons. In general terms, a breach will occur whenever any personal data is lost, destroyed, corrupted or disclosed. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. loss or theft of a computer, portable device, such as a laptop or data stick)
- Unauthorised access to, use, or alteration of, personal data
- Deliberate or accidental action (or inaction)
- Loss of availability of personal data (e.g. encrypted by ransomware, or accidentally lost or destroyed) or through equipment failure (e.g. data cannot be accessed and is not backed up)
- 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

3. What should I do when a breach occurs?

Should a breach occur, it is extremely important to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and to help prevent any recurrence.

Members of the University should report any breach or suspected breach to their School or Service's Data Protection Champion and to the University's Data Protection Officer (DPO) immediately upon becoming aware of it:

DPO: Rebecca McCall, University Solicitor; email: data.protection@hud.ac.uk; tel: 01484 473 000

The DPO will deal with the breach. In their absence a breach 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 DPO will follow when they are made aware of a data security breach.

3.1 On discovery of a breach

Following receipt of a report of a suspected breach the DPO will confirm whether a breach has occurred and assess the risks associated with it. They will ask the person reporting the to complete the Data Protection Breach Evaluation Form. The Data Protection Champion for the relevant School/Service will assist with this process.

The DPO will update the Data Breach Log, which is maintained by the DPO.

Following evaluation of the breach, the DPO will contact the Data Protection Champion (copied to their Dean/Head of Service) for the relevant School or Service concerned to explain:

- the nature of the breach
- an indication of the seriousness of the breach
- any action the School or Service must take immediately (i) to contain the breach and (ii) to become compliant with the GDPR/DPA and/or (iii) to prevent a similar situation from arising in the future. If the breach is a continuing breach, steps must be taken immediately to minimise the effect of the breach, e.g. to shut down a system or alert relevant staff.

The DPO will continue to monitor the situation to ensure that the School/Service responsible for the breach completes any required actions as soon as possible.

3.2 Managing the consequences of a breach

Depending on the seriousness of the breach and following guidance issued by the Information Commissioner's Office, the DPO may:

- inform the University Secretary
- inform the Information Commissioner's Office (this is mandatory where there is a risk to people's rights and freedoms)
- inform the Director of Marketing and Communications if there is potential for press interest
- inform the data subjects affected by the breach

3.3 Preventing a repetition of a breach

After completing the procedures set out above, the DPO will evaluate the breach 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 a breach from recurring and will publicise internally any learning outcomes from

their investigation of a breach, including via Information Governance Group, Data Protection Champions and SMT, as appropriate.