H

1. DATA PROTECTION POLICY

for example agents, external organisations, consultants, contractors and service providers who process Personal Data on behalf of the University.

5. Data Security

5.1 As a data controller, Harper Adams University has a responsibility under Article 24, to ensure that there are appropriate technical and organisational measures in place to ensure that all data processing is performed in accordance with data protection law. The University must keep all Personal Data (including Special Category Data)

explain any research and in some cases to obtain their consent. Please speak to the Data Protection Officer if you wish to convert Personal Data into anonymous or pseudonymised data or use it for research before doing so, or if you have any concerns about current use.

7.0 Lawfulness of processing data

7.1 One of the main data protection obligations requires the University (and its employees) to process Personal Data lawfully, fairly and in a transparent manner. This means under Article 6 that the University (and each employee) must comply with at least one of the following conditions when processing Personal Data:

- the individual to whom the Personal Data relates has consented to the processing;
- the processing is necessary for the performance of a contract between the University and the individual;
- the processing is necessary to comply with a legal obligation placed on the University;
- the processing is necessary to protect a vital interest of the individual

10.3 In addition,you must take care to record and input Personal Data accurately. This is important. There can be serious risks for the University if Personal Data is incorrect. Some Personal Data may

13.2 A data subject can request from the University to:

- Confirm whether or not their Personal Data is being processed, the purpose of the processing and categories of data processed
- Have access to that data (a copy is normally provided)

The data subject may also request:

- The recipients or categories of recipient to whom the Personal Data have or will be disclosed, in particular recipients in third countries or international organisations,
- Where possible the envisaged period for which the Personal Data will be stored, or the criteria used to determine that period,
- The existence of the right to request rectification or erasure of Personal Data or restriction from processing of Personal Data concerning the data subject, or to object to such processing,
- The right to lodge a complaint with the ICO,
- Where the data was not collected form the Data subject, any available information as to the source,
- Where Personal Data are transferred to a third country or an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer,
- Information on the existence of any automated decision making, including profiling; and
- To be provided with copies of the Personal Data held about him or her

14.0 Data loss or security breach procedure

14.1 There are potentially significant repercussions for the University and the individuals affected arising from a data loss or security breach. Where this occurs or you suspect it may have occurred you must:

- Immediately report the details to the Service Desk. If they are not available then you must contact the Data Protection Officer and Service Delivery Manager providing them with as much information as you have available;
- It is important that this is done as quickly as possible as it may be possible to reduce the impact of the breach by remote deletion, removal or other means.
- Follow their guidance on dealing with the security breach and keep them up to date with any further information about it that you become aware of;
- Not approach any individual data subjects, suppliers, regulators or make any public announcements about the security breach incident without the prior agreement of the University Secretary.
- Also see Data Breach Procedure at Appendix 1 to this Policy.

14.2 The member of staff responsible for the data breach must undertake a mandatory data protection course as directed by the DPO. The course must normally be completed within 2 weeks of the date of the report of the data breach but up to a maximum of 4 weeks if agreed by the DPO and the relevant line manager. It is the member of staff's responsibility to inform the DPO and the Organisation Development Manager once the course has been completed. Failure to complete the course in the time agreed could be viewed as a disciplinary issue.

15.0 Disclosure of data

15.1 Any

17.2

19.0 Data Protection Impact assessments

19.1

Data Breach Flowchart

Staff member must report to their line manager immediately or their absence report

Consider whether any steps can be taken to minimise or mitigate the data loss, including informing the data subjects.

1.7 It is important that assessment of the incident, its management and outcomes are considered in order to improve this procedure and the handling of data security breaches. The DPO and SDM should consider whether there are any learning outcomes from each incident.

2.0 Policies applicable

2.1 In order to comply with the Data Protection Act 2018 and the UK GDPR, organisations which process personal data must take approprw 1j4(D)-1.62.5(m)9o3.3(d)-2su1.7

4.2 Special Category Data: a sub-category of personal data (previously known as sensitive personal data) is Personal Data about a person's race or ethnicity, their health, their sex life or sexual orientation, their religious or philosophical beliefs, their political views or trade union membership, their physical or mental health or condition, genetic or biometric data.

4.3 Data subject: The person whom the data concerns

4.4 Disclosure: Personal data should only be disclosed within the University to members of staff who need to know it in order to carry out their duties, or to others connected with the University who have been approved to receive such information in relation to university activities or events.

5.0 Roles and responsibilities

5.1 Staff who experience or discover a data loss are responsible for reporting it immediately and should know to whom they should report or escalate an incident. This will normally be their line manager. The line manager should immediately report the incident to the Service Desk. If the line manager is not available then the staff member should report the incident to the Service Desk themselves, as a matter of urgency.

5.2 Students should normally report incidents to their tutor or supervisor, who will be responsible for onward reporting of the incident to the Service Desk. Most instances of students processing personal data are not within the scope of the UK GDPR as personal use of data is not governed by the UK GDPR.

5.3 The incident owner will normally be the Data Protection Officer or Service Delivery Manager

6.3 If in doubt, it is better to report a suspected incident than to ignore it

6.4 On becoming aware of a data security breach there may be immediate actions you can take to contain or lessen the impact. In the situations described, these could include

- Immediately recalling an incorrectly sent email. Or, if the recall is unsuccessful, by contacting the person/people to whom personal data has been disclosed, apologising and asking them to securely delete it from their systems (including from deleted items folders) and to immediately confirm that they have done so
- Immediately retrieving paper documents from any unintended recipients
- Immediately disabling any lost or stolen data storage devices.

7.0 Information Gathering

7.1 It is the responsibility of all staff involved in any data loss or breach to gather enough information to determine whether or not a data breach has actually occurred and the urgency of response required. If in any doubt the Data Protection Officer and the Service Delivery Manager can offer advice on the type of information required to make a reasoned decision.

sMran7(d-5 [(o)2l0dy-1.2)7.4(r)-ET-5.(s)MaBT-5CS1 cs5-3.3584 obs-3.3584m]TJ -oJu038n-3.3358ys(oJu038n-s-3.3358

9.0 Actions and notifications

9.1 Any further actions to be taken will be determined following the investigation
9.2 The communication

11.0 Examples of incidents that should be reported

11.1 IF UNSURE, REPORT IT.
ALL INCIDENTS SHOULD BE REPORTED TO THE IT SEVICE DESK ON EXT 5555.

11.2 The Incident Report Form below, will be completed by the Service Desk. It is attached so that staff are aware of the type of questions they will be asked when reporting a data breach.

11.3 Examples of data breaches that should be reported to the Service Desk:

- Misdirection of emails or correspondence containing personal data,
- Sending non-essential personal data to otherwise valid recipients,
- Failure of access controls, such as incorrect allocation of permission or password sharing, which result in unauthorised access to personal data,
- Loss or theft of papers containing personal data,
- Incorrect permission levels on folders containing personal data,
- Personal data received in error,
- Publication of personal data on a website,
- Loss or theft of any university owned data storage device regardless of the data it contains e.g. laptop, PC, USB/pen drive, iPad or other tablet, removable hard drive, smart phone or other portable devices,
- Hacking or unauthorised access gained to University IT systems,
- Theft of any privately owned devices should only be reported if they contain personal data related to university activities. Use of private devices should be avoided for University purposes,

5. What are the risks or likely consequences of this data breach? [Consider risks to data subjects, risks t University]
6. Have any steps been taken to retrieve or delete the data? Is it possible to take any steps to reduce th of the loss on the data subjects?

Please consider these options:

Can an email be recalled? Yes No

Next Sections are for completion by DPO only

9. Risk assessment of the breach (see factors here)
10. Following the risk assessment, does the incident require notification to the ICO? (required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals)
Yes δ No δ Completed δ Do the data subject(s) need to be informed? Yes δ No δ Completed δ
11. Details of investigation by DPO
12. Learning outcomes of the investigation
13. Incident closed with Service Desk? Yes δ No δ

14. Has staff member been passed to Staff Development Officer for DP Training?	Yes δ No δ
15. Has he training been completed?	Yes δ No δ