
H

Data Protection Policy

Index

1. DATA PROTECTION POLICY.

1.1. This Data Protection Policy ("the Policy") regulates the way in which Harper Adams University ("the University", "we") obtains, uses, holds, transfers and otherwise processes Personal Data about individuals and ensures all of its employees know the rules for protecting Personal Data. Further, it describes individuals' rights in relation to their Personal Data processed by the University.

1.2. The University abides by UK data protection laws, including the Data Protection Act 2018 ("the DPA") and the U.K. General Data Protection Regulation ("the UK GDPR"), in its handling of Personal Data. All references within this policy refer to the UK GDPR 67(R)]3.6(o.003 1.357.9(io)0.0)Tj7(.0.0 8.0.3

5. Data Security

5.5 Please note that it is the University's policy not to permit auto-forwarding of University email boxes to personal email boxes. This applies to both staff and student email. This does not prevent staff/students reviewing emails on their personal devices such as smart phones. All devices, whether University owned or personal devices being used for work emails, should be password protected and have appropriate security settings to permit effective remote destruction if lost. Please contact services desk for advice. All University devices must have security systems added by service desk and staff using such devices are responsible for checking with services desk that these security arrangements are in place on any University owned device they are using. Staff are personally responsible for ensuring appropriate security of their own devices if they use them for accessing work emails. Staff are encouraged only to use University devices for work purposes wherever possible and preferably to use remote desk top worki

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:

; D2(n)(pr0 j0 i-00/T ac)(t)9ny(4--5. n/TT0 1)]-8(i.1(t)9nTc0.7p)(al ()-7x7Tc0.7bu6.1(ITc0.7I707 h)w-53(9())Tj8(. F)2.

- 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 or another person;
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the University.

7.2 The individual's consent to processing Personal Data should only be relied upon where there is no other lawfu-0.003 Tcor
it3.1(al 4(-14 -4OTc 0x)10.6(e)-4(r)-5.3(c)0.)11.9(t)-7.9(e)-4( )11.1(U)-7 Tc 0.210.216

8.0 Special Category Data

8.1 Special Category Data (also known as sensitive processing) is Personal Data about a person's race

9.0 Privacy notices

9.1 If the University is collecting Personal Data from people, then it must at the time of collection, provide them with certain information in what is called a Privacy Notice. The ICO has published guidance on Privacy Notices which may be viewed on their website.

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 change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date. If not, there may be serious problems. For example, a renewal or termination notice for a contract may be sent to the wrong address and may not be valid.

11.0 Data retention

11.1 The University cannot keep or retain most Personal Data forever. Some records have to

Therefore, please inform the Data Protection Officer immediately and follow their instructions. You must not deal with such requests in isolation.

13.2 A data subject can request from the University to:

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 disclosure of Personal Data is a form of processing. That means that the rules described above concerning fair and lawful use must be satisfied. You must not disclose Personal Data to a Third Party outside the University unless that disclosure constitutes a lawful reason for processing and satisfies the information notice requirements as explained above. The Data Protection Officer will be happy to discuss this with you. In particular, it is important to note that Personal Data and Special Category Data so1

17.0 Data collection for marketing purposes

17.1 The collection of Personal Data for marketing purposes is largely governed by the Privacy and Electronic Communications Regulations (PECR). These may be viewed here. Advice from the ICO on PECR may be obtained here.

17.2 Where the University intends to collect the Personal Data of people and use it for marketing purposes, this must be clearly stated in the data collection notice and the person must give clear, informed and specific consent to show that they understand what they are being asked to consent to. This will normally be by a series of tick boxes allowing the person to select how they wish to be contacted. This is known as 'opting in'. Opt-out and pre ticked boxes are no longer allowed and are not acceptable.

17.3 Forms collected recording a data subject's consent to be contacted for marketing purposes should be retained and stored for as long as the University is sending them any marketing information. This may only be destroyed once the marketing relationship has finished. Under Article 21 data subjects have the right to object to having their data processed for direct marketing purposes and so are entitled to ask to be deleted from any contact lists.

18.0 CCTV

18.1 For reasons of personal security and to protect University premises, the property of staff and students, overt CCTV cameras are in operation across the campus.

18.2 Appropriate signage is in place at the perimeter and around the University campus stating that CCTV is in use.

18.3 The objectives for the use of the CCTV system is to:-

- Assist in providing a safe and secure environment for the benefit of those who might visit, work or live on the campus.
- Reduce the fear of crime by reassuring students, staff and visitors.
- Deter and detect crime, public disorder and anti-social behaviour.
- Identify, apprehend and prosecute offenders in relation to crime, public disorder and anti-social behaviour.
- Monitor and assist with traffic management.
- Assist in the monitoring and deployment of security staff during normal duties and emergency situations.
- Protect security officers from undue threats and violence.

18.4 In addition to data protection laws, CCTV is covered by the following legislation:

- Regulation of Investigatory Powers Act 2000.
- Protection of Freedoms Act 2012
- Surveillance Camera Code of Practice, Pursuant to Section 30 (1)(a) of the Protection of Freedoms Act 2012.

18.5 CCTV is subject to the same Subject Access Request rules as written data. Any person wanting copies of their data should contact the Head of Security in the first instance.

18.6 Access to the live feed and images stored on the CCTV system is restricted to trained personnel, in accordance with the University CCTV Code of Practice. It is normally deleted after 14 days unless retained for an incident requiring further investigation.

19.0 Data Protection Impact assessments

19.1 Data Protection Impact Assessments (or Privacy Impact Assessments as they are sometimes known) are a tool to help organisations identify the most effective way to comply with their data protection obligations and to meet individuals' expectations of privacy. DPIA's should be considered whenever data processing is 'likely to result in high risks for individuals.' It is a process that will help the University to identify and reduce the privacy risks of a project or process.

19.2 DPIA's should be conducted at an early stage in a project to allow for the assessment to influence and if necessary change the project, taking full account of privacy issues.

19.3 A DPIA involves the examination of all data information flows and minimising any risk associated with the collection, retention, use and destruction of the data. DPIA's also include an examination of the necessity and proportionality of any data collection process and should also examine privacy issues associated with the project. This may include issues such as who has access to data, the organisational and technical measures in place to provide data security, intrusion into people's lives and steps taken to minimise these issues. Consultation with stakeholders and those affected must also be taken into account.

19.4 Examples of projects that may benefit from a DPIA include:

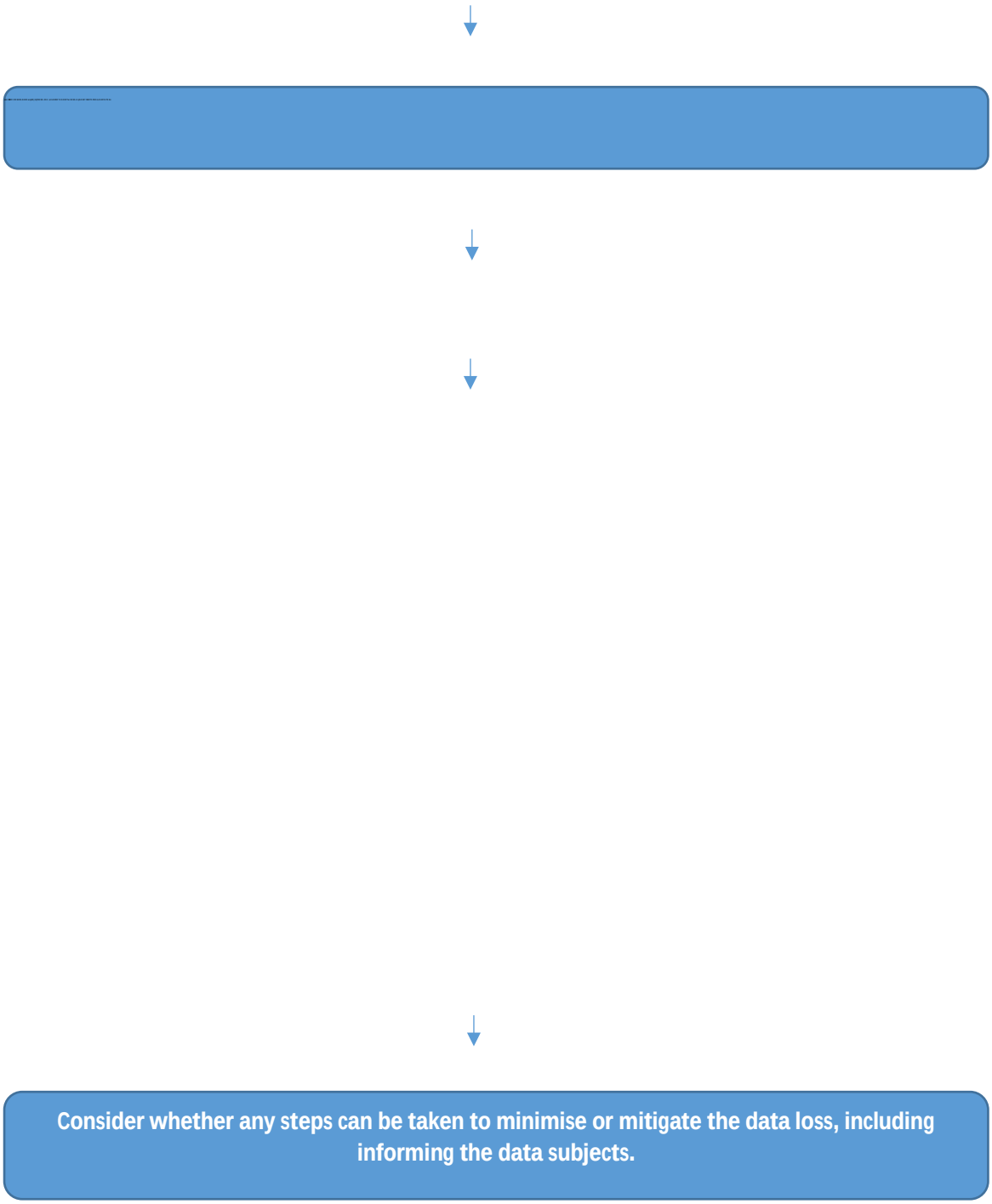
- Installation of new or additional CCTV cameras or systems
- A new database to record staff or student data
- A project to identify stutd0.0787 Tc 0.002.7(o22.3(f)-3.a p(da)117(ur)6llat)-7.-4(c)0.la.3(r)-5.gro oe4 cossurseof alAtas on.

x A newossnala n o13.8((o)-0.3(r)-69(o)1j(IA-0.7(e)c13(t).9( )11.1(t.t)-9(o)1.p5(n)103(r

Data Breach or Loss - Assessment and Reporting Procedure

Contents

Data Breach Flowchart



1.7

can also include an online identifier or one or more factors specific to the physiological, genetic, mental, economic, cultural or social identity of an individual.

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

.

exposure. If an incident occurs or is discovered outside of normal working hours, it must be reported as soon as is practicable

9.0 Actions and notifications

9.1 Any further

11.0

Appendix 1
V1.3

Data breach or loss report form to be completed **by Service Desk only**.

Please forward to dpo@harper-adams.ac.uk ASAP once completed

Service Desk Ticket No.	IN
IT Service Desk member taking the report	
Time and date of report	
Time & date that the incident occurred	

4. What were the causes of the incident?
5. What are the risks or likely consequences of this data breach? [Consider risks to data subjects, risks to the University]
6. Have any steps been taken to retrieve or delete the data? Is it possible to take any steps to reduce the impact of the loss on the data subjects?
Please consider these options: Can an email be recalled? Yes δ No δ Can an email be deleted from the inbox of the incorrect recipients? Yes δ No δ If a system has been hacked or if there is unauthorised access to a system or folder, can this system be immediately turned off until correct permissions are applied to it? Yes δ No δ Is it possible to remotely delete or wipe the lost article? Yes δ No δ
7. Any other information, factors or views that investigators should be aware of? [Is the data subject aware of the breach? Do not disclose the breach

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)