Data Protection Policy

(Including data breach procedure)

Harper Adams University

December 2018

Data Protection Policy

Index

If you have any questions about the use of data or would like to know more about the legislation governing the use of data please contact the Data Protection Officer at dpo@harper-adams.ac.uk or on extension 5340.

1.0 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 General Data Protection Regulation ("the GDPR"), in its handling of Personal Data. All references within this policy refer to the GDPR and the DPA 2018.

1.3. We aim to ensure our employees are acting in accordance with these laws and the relevant regulatory guidance and any available best practice. Those requirements, together with this Policy, ensure that all employees of the University fully understand the University's obligations to comply with the DPA, GDPR and other privacy laws and regulations of the UK. In order to ensure that all staff have had some basic training in data protection requirements, all staff who have routine access to a computer, will be required to undertake the University online Data Protection Training annually.

1.4 Where the University controls other entities (whether by virtue of contract, partnership, ownership of shares or otherwise), those other entities will be required to abide by the principles set forth in this Policy. References to "you" are to individuals who process Personal Data (as defined below) on behalf of the University in accordance with this Policy.

1.5 Please note that reference is made throughout this document to the Data Protection Officer, Christopher Munro dpo@harper-adams.ac.uk. In his absence, advice may be sought from the University Legal Advisor, the University Legal Officer or the University Secretary.

1.6 This Policy is written in accordance with both the GDPR and the Data Protection Act 2018. The GDPR has direct effect across all EU member states and this means that organisations will still have to comply with this regulation and we will still have to look to the GDPR for most legal obligations. However, the GDPR gives member states limited opportunities to make provisions for how it applies in their country. These are referred to as derogations. One element of the DPA 2018 is the details of these derogations. It is therefore important the GDPR and the DPA 2018 are read side by side.

2.0 Personal Data

2.1 "Personal Data" is defined in Article 4 as any information (for example, a person's name) or combination of information about a living person which allows that living person to be identified from that information (for example a first name and an address). Personal Data 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.

2.2 Examples of Personal Data which may be used by the University in its day to day business include names, addresses (e-mail and postal addresses), telephone numbers and other

contact details, CVs, performance reviews, payroll and salary information, health information and financial information. The definition also includes opinions, appraisals or intent regarding individuals (e.g. employees, job applicants, students, personal contacts at suppliers and individual members of the public).

2.3 The laws governing how we can use Personal Data apply whether the Personal Data is stored electronically (for example, in e-mails, on IT systems, as part of a database or in a word processed document) or in structured manual records (for example, in paper files or filing cabinets).

3.0 Data Processing Activity

3.1 Harper Adams University is defined as a Data Controller under the GDPR. The University collects and processes Personal Data on its students, employees, agents, the employees of its suppliers and any other individuals, including applicants and former employees, for a multitude of purposes, including:

- Maintenance of the Student record
- Recruitment;
- Employee performance management and professional development;
- Payroll, fund management and accounting;
- Business and market development;
- Building and managing external relationships;
- Research and development;
- Planning and delivering of education and training;
- Staff and student support and facilities management;
- Knowledge management;
- Health, safety and security; and
- Other purposes required by law or regulation.

3.2 When we collect, record, store, use, adapt, share or erase Personal Data for any of these purposes, this is called processing, including if it is carried out by automated means. If you read, amend, copy, print, delete or send Personal Data to another legal entity (i.e. outside the University) this is a type of "processing" and is subject to the guidelines set out in this Policy.

4.0 Data Protection enforcement

4.1 Within the UK, data protection laws are enforced by the Information Commissioner's Office ("the ICO"). The ICO can investigate complaints, audit the University's processing of Personal Data and can take action against the University (and you personally in some cases) for breach of the DPA, GDPR and other relevant privacy laws. Such action may include fines (of up to €20m), permanently or temporarily limiting processing, warnings and reprimands. Additionally, organisations which are found to be in breach of the DPA, GDPR and other privacy laws also often receive negative publicity for the breaches which can affect the reputation of the University as a whole.

4.2 Each University staff member or Third Party is required to read and comply at all times with this Policy. In this Policy a "Third Party" is anyone who is not an employee of the University, for example agents, external organisations, consultants, contractors, and service providers who process Personal Data on behalf of the University.

5.0 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) secure. This means that the Personal Data must be protected against being accessed by other companies or individuals (for example, via hacking), from being corrupted or being lost or stolen. The Personal Data must also be protected so the wrong people cannot read or use the details. This applies to details in IT systems, e-mails and attachments and paper files. This is why, for example, you have a password and controlled access rights to IT systems. You must comply with the University's security procedures whenever you handle Personal Data. The University relies on you to keep data secure and for data security and to comply with the University's Acceptable Use Policy.

5.2 It is the University's policy that any University work (whether personal data or otherwise) must only be saved on an encrypted portable device obtained from the Service Desk. This includes lecture notes, presentations etc. Rather than use memory sticks, flash drives or CDs or similar portable data devices, the University expects staff working away from their own office/desk while on the University's campus to log into the University's network and access materials directly from the University's PCs. PCs are for example located in all teaching spaces so that staff delivering teaching sessions do not need to carry data devices around the campus. Where the Service Desk has advised that a large data source is such that it can only be accessed from a portable device, an encrypted device provided by the Service Desk must be used at all times. (note: The University's IT team are working towards enabling access to large data sets from all on-line points during the first quarter of 2019 and staff will be updated when this is available. In the meantime staff must use log in access as much as possible, as noted above, and always use only encrypted devices where it is not yet possible to use direct log in access.)

5.3 If you work away from the University's premises, you must comply with any additional procedures and guidelines issued by the University for home working and/or offsite working particularly, as this presents a potentially greater risk of loss, theft or damage to Personal Data. You must read these procedures and guidelines before processing any Personal Data away from the University premises. Please ensure that any data of any kind related to your work at the University, whether teaching materials, presentations or any other data category is always carried only on an encrypted device.

5.4 Extra care is needed to secure Special Category Data because more damage is likely to occur if it is lost. For example, if details of an individual student's medical conditions got into the wrong hands it would be very distressing for that student. Be especially careful if you want

to send Special Category Data to another person, including by email, that it is sufficiently secure and can only be received and accessed by the intended recipient. Email attachments should be encrypted. If in doubt, seek guidance from the Data Protection Officer or the Chief Technical Officer in relation to IT security. Do not load Personal Data of any kind onto unencrypted storage devices such as memory sticks, flash drives or CDs.

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 working. Contact Services desk for advice.

5.6 The University also recognises that adequate security is important where it arranges for outside service providers to process Personal Data on its behalf. Where such arrangements are established by the University, service providers must be bound by written contracts to protect the Personal Data provided to them. See the section below for more information.

6.0 Records of Processing

6.1 Under the GDPR Article 30 (5) organisations of more than 250 employees must maintain records of their processing activities. This is to replace the previous registration with the ICO. The following information will be recorded.

- Name and details of Harper Adams University, other data controllers and the Data Protection Officer.
- Purposes of processing
- Descriptions of the categories of individuals and categories of Personal Data.
- Categories of recipients of Personal Data
- Details of transfers to a third country including documentation of the transfer mechanism safeguards in place.
- Retention schedules
- Description of technical and organisational security measures.

6.2 We may be required to make these records available to relevant supervisory authorities for purposes of investigation.

6.3 If you begin carrying out new data processing activities, please contact the Data Protection Officer immediately to discuss the details with them first in case any processing description needs to be updated.

6.4 In order to avoid processes changing without the knowledge of senior management, your assistance in keeping this information up to date would be gratefully appreciated. The Data Protection Officer is dependent upon you for this information.

6.5 It may in some cases be possible to convert Personal Data into anonymous Personal Data or pseudonymised data, such as aggregated statistical data where data subjects cannot be identified, or to use it for research provided its use will not impact or affect any data subject individually. However, it may be necessary to have warned data subjects in advance that this might happen, to 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 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 lawful reason to process data. Additional stringent conditions apply to reliance upon consent; please discuss this with the Data Protection Officer.

7.3 Article 4 also defines the principles relating to the processing of Personal Data:

- Personal Data should only be collected for specific, explicit and legitimate purposes. It should not be further processed in a manner which is incompatible with the stated purposes.
- The Personal Data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Personal Data must be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that are inaccurate are erased or rectified without delay.
- Personal Data must not be kept for longer than is necessary for the purposes for which it is processed. Contact the Data Protection Officer if you have any concerns about data retention.

7.4 If in any doubt about the lawful, fair and transparent use of Personal Data, you should contact the Data Protection Officer.

7.5 If you want to make a new use of any Personal Data held by the University, you must not do so unless that new use satisfies one of the lawful reasons for processing and it is described in the relevant privacy notice provided to an individual (see below). For example if someone provides their Personal Data as a parent / guardian for student support purposes, you may not be able to start sending them marketing e-mails unless that is covered in an appropriate privacy notice and accompanied by explicit consent from that individual.

8.0 Special Category Data

8.1 Special Category Data (also known as sensitive processing) 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.

8.2 Processing of Special Category Data is prohibited unless the processing is lawful under the categories described above and also, one of the following applies:

- The individual has given explicit consent to the processing for one or more specified purposes;
- The processing is necessary for the purposes of carrying out obligations or specific rights of the University in relation to employment, social security and social protection law;
- The processing is necessary to protect the vital interests of the individual or another whether the individual is incapable of giving consent;
- The processing is carried out in the course of legitimate activities (with appropriate safeguards) by a foundation, association or other not-for-profit body with a political, religious, philosophical or trade union aim. The processing must relate solely to members or former members or individuals who have regular contact with it in relation to its purposes. The Personal Data must not be disclosed outside of the body without consent.
- The processing related to Personal Data which has been made public by the individual;
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of working capacity of the individual, medical diagnosis, provision of health or social care treatment or the management of health or social care systems and services;
- Processing is necessary for reasons of public interest in the area of public health;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

8.3 Special Category Data on staff or students should not be collected or otherwise processed unless it is essential to do so. Extra care must be taken with it (in addition to the normal rules for Personal Data) and it must be kept more securely. Additional restrictions are placed on top of the lawful reasons for processing mentioned above. For example, consent of the individual has to be explicit, specific and informed and obtained prior to processing any Special Category Data.

8.4 The University does not generally seek to obtain Special Category Data unless:

- the individual concerned agrees in writing that the University may do so, on the basis of a full understanding of why the University is collecting the data; (this will be the case for Learner Support and also counselling services offered to students)
- the University needs to do so to meet its obligations or exercise its rights under employment law; or
- in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned or staff, students or visitors.

8.5 Employees should note that the "legitimate interest" criteria described above is not valid when processing Special Category Data. Special Category Data should not be collected for any new purposes without the involvement of and advice from the Data Protection Officer.

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 here.

9.2 In accordance with Article 5, any processing of Personal Data must be undertaken lawfully, in a fair and transparent manner. In accordance with Article 13, the University must provide the data subject with a Privacy Notice and provide certain information within that notice including:

- Name and contact details of the person collecting the Personal Data and the University DPO,
- The purpose and legal basis for processing the data,
- Any disclosure or sharing with third parties,
- Whether it will be transferred out of the country

9.3 You should therefore check whether there is an applicable notice which covers the processing you intend to carry out for the University. Personal Data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

9.4 The University must also provide the individual with information on the period for which the Personal Data will be stored, the individual's rights on rectification, erasure and data portability, whether automated decision making or profiling will be carried out and the right to withdraw consent to processing if that is relied upon as the lawful basis for processing.

9.5 If you have any questions about privacy notices, or wish to undertake a new project which involves a change in the way individuals' Personal Data is processed by the University, please contact the Data Protection Officer.

9.6 The University must comply with all the rules of processing contained within the GDPR. These will include:

- the data being adequate, relevant and not excessive,
- accurate and where necessary kept up to date,
- kept for no longer than is necessary,
- processed in a way that ensures appropriate security of the data, using appropriate technical and organisational measures,
- Personal Data must not be used in a way which would infringe another law. For example for bribery, or discrimination on the basis of race, age, sex, or disability.

9.7 Where collecting Personal Data about an individual indirectly (e.g. from a published source), the University must still inform the individual that it holds the data and the purposes for which that data will be used.

10.0 Processing relevant data and keeping it accurate

10.1 Personal data collected shall be adequate, relevant and limited to what is necessary for the purpose for which it is processed. You must not collect and process more Personal Data than you need. For example, if you will never telephone someone at home, you do not need to record their home telephone number.

10.2 Personal Data (including any Special Category Data) you collect should be appropriate to, and sufficient for, the relevant purpose(s) you are collecting it for, but not excessive for that purpose(s). You must only process the data which is necessary for the task.

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 be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws). Other records must only be kept while in current use and for a reasonable period afterwards. All staff must comply with the University's Record Retention Schedule relevant to their own area of work. The University record retention schedule is published as part of the Publication Scheme and is available here.

11.2 As a general rule, when Personal Data is no longer needed by the University for the purposes for which it was collected, this Personal Data should be securely destroyed as soon as practicable.

12.0 Data subjects rights

12.1 Individuals have certain rights in relation to their Personal Data:

- the right to access Personal Data held about themselves;
- the right to prevent processing of Personal Data for direct marketing purposes;
- the right to have Personal Data rectified if it is inaccurate;
- the right to have their Personal Data erased (the 'right to be forgotten');
- the right to restrict processing in certain circumstances;
- the right to data portability in certain circumstances;
- the right to compensation for any damage/distress suffered; and
- the right to be informed of automated decision making about them and the right to object to such processing and to not be subject to automated decision making which produced legal effects concerning the individual.

12.2 If you should receive an enquiry about any of the above rights that you are unsure about, then you should seek advice from the Data Protection Officer.

12.3 Individuals are allowed to withdraw their consent to the University's use of their Personal Data at any time. However, the University will only be relying on consent to process Personal Data in very limited circumstances. Other lawful reasons for processing will be relied upon where possible. If an individual contacts you to withdraw consent, inform the Data Protection Officer promptly to seek advice and stop using / processing that Personal Data in a way that is inconsistent with the withdrawal of that consent until you have received guidance from the Data Protection Officer as to the necessary steps to be taken.

13.0 Subject access requests (SAR's)

13.1 Under Article 15 individuals can ask for copies of the Personal Data the University holds about them and other details about how the University uses their Personal Data. If you receive such an access request, there are special legal rules which must be followed as part of this process. 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:

- 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.

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 have to 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 on students must not be disclosed to parents/guardians without consent (and in the case of Special Category Data, written consent) to that disclosure being obtained from the student in advance. This is the case regardless of whether the student is over 18 or under 18. Such disclosures are likely to be a breach of the GDPR. If there is an emergency or another urgent situation in which you feel it is necessary to disclose Personal Data (or Special Category Data) to a parent/guardian

without consent being obtained, please liaise with the Data Protection Officer to confirm that it is lawful to disclose in those circumstances.

15.2 There are some other exceptions to deal with disclosures such as those requested lawfully by police where the information is necessary to prevent or detect a crime. If you receive a request for information about an individual from the government, police or other similar bodies or from other investigators you should pass that request immediately to the Data Protection Officer to be dealt with. The application of the relevant exceptions needs careful consideration. The burden is on the University to determine whether these apply. Disclosure will normally require that the police complete a form A221 before disclosure. This form may be obtained from the police, DPO or Head of Security.

15.3 Third parties and contractors should only have access to data as required by their job role. They are also bound by rules of confidentiality concerning access to Personal Data.

16.0 Transfer of data to third countries or international organisations

16.1 The GDPR contains special rules on whether Personal Data collected in the UK can be transferred to another country. Within the UK, there are restrictions on the transfer of Personal Data outside of the European Economic Area (such a transfer can happen, for example, where Personal Data is e-mailed outside the EEA). This is to make sure the Personal Data remains safe and the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

16.2 The fact that there will be transfers of Personal Data to other countries, especially to outside the EEA, should be clearly set out in the privacy notices described in the fair use section of this Policy above so that it is expected by the affected individuals.

16.3 Articles 44 – 50 GDPR cover the law regarding the transfer of data outside the EEA. For more information on overseas transfers please contact the Data Protection Officer.

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.
- Provide the Police, Health and Safety Executive and University with evidence upon which to take criminal, civil and disciplinary action respectively.
- 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 students of a particular group or demographic which may initiate a course of action.
- A new building project to provide student accommodation
- A new database to consolidate several existing databases containing student or staff data

19.5 Please note that under the GDPR non-compliance with requirements to conduct a DPIA may lead to enforcement action by the ICO. These assessments are no longer optional and just good practice, but are an essential part of documenting how the University complies with its responsibilities under the GDPR.

Dr C E Baxter

University Secretary

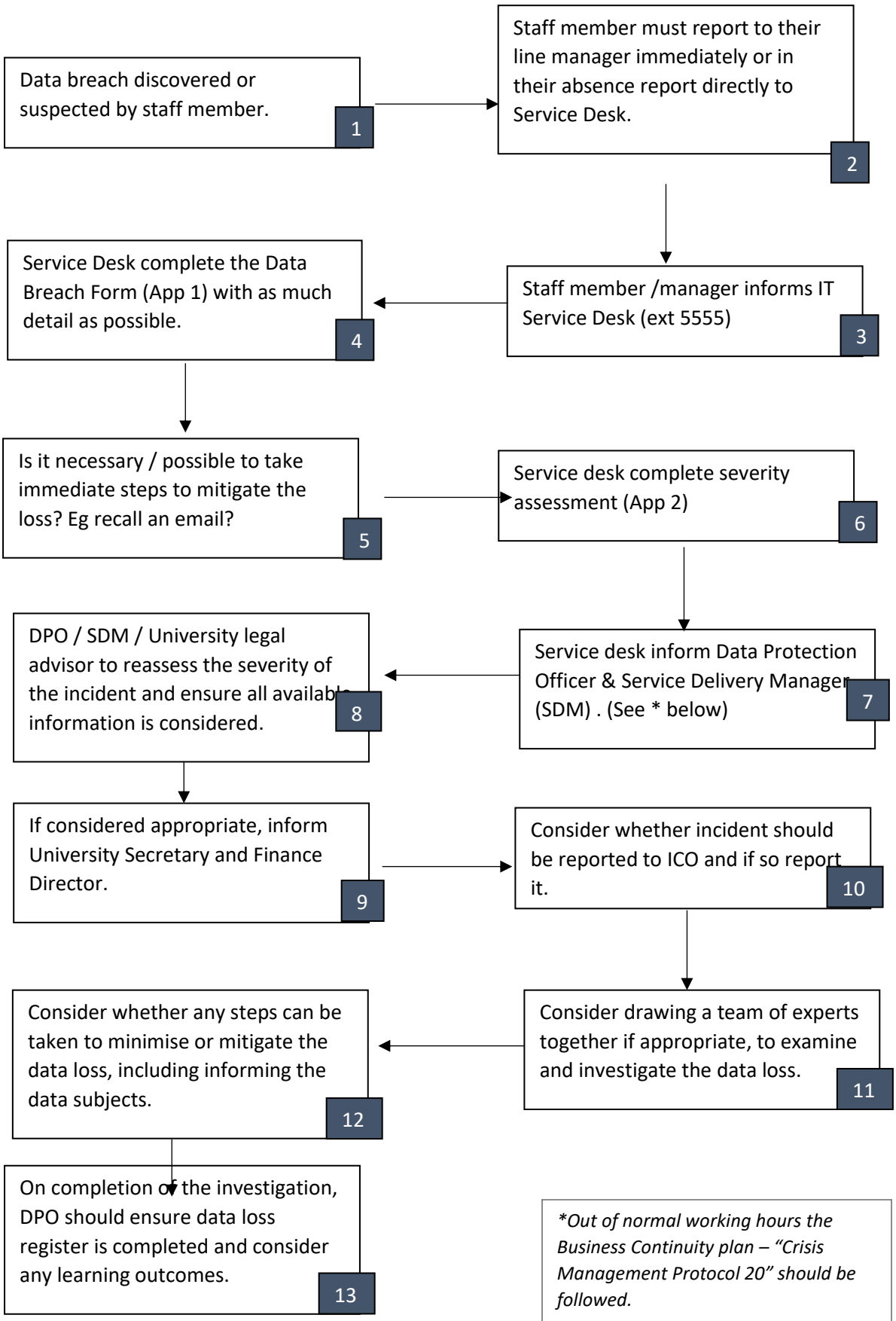
12th September 2018

Data Breach or Loss Assessment and Reporting Procedure

Harper Adams University

Contents

Process Flowchart



1.0 Background to the procedure

1.1 This Procedure covers any incident where it appears that personal data for which the University is responsible is lost, misused, wrongly or unlawfully disclosed or accessed, or there is a risk that an incident may allow unauthorised access to personal data. An incident may include (but is not restricted to) the following:

- Loss or theft of personal data, special category data or equipment on which this kind of data is stored
- Equipment theft or failure containing personal data
- Unauthorised use of, access to or modification of data or information systems
- Attempts (whether successful or not) to gain unauthorised access to data or IT systems
- Unauthorised disclosure of personal data or sensitive personal data
- Hacking attack or viruses
- Human error
- Attempts to obtain data by deception

1.2 This procedure should be read in conjunction with the ICO Guidance on Breach Management and the Article 29 Working Party guidelines here. There is also advice on how and when to report incidents to the ICO available on their website here. A copy of the breach notification form is available here.

1.3 If as a result of the investigation into a data breach, it becomes apparent that a staff member has been negligent and that that this was a contributory cause which lead to a breach of the Data Protection Act 1998 or General data Protection Regulation then this may lead to a formal misconduct procedure being initiated.

1.4 Any staff member who becomes aware of an obvious data breach and does not report it may also have disciplinary proceeding initiated as a result of failing to act.

1.5 At Appendix 1 there is form for completion by the Service Desk and the Data Protection Officer or in his absence the University Legal Advisor, including determining whether a breach should be reported to the Information Commissioner's Office (ICO).

1.6 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 GDPR, organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of, or damage to personal data.

Where such measures fail, this Data Loss Assessment and Report Procedure must be followed.

2.2 The requirements of this Procedure must be applied in conjunction with all applicable University policies and procedures, including:

- The Data Protection Policy
- IT Acceptable Use Policy
- Academic Staff Handbook
- Support Staff Handbook

3.0 Purpose

3.1 The purpose of this document is to describe the procedure for reporting incidents which involve the actual or suspected disclosure of personal data (as defined below) to unauthorised persons. It applies to all personal data made available to the university, irrespective of the source of the data or the media upon which it is held, and encompasses all university activities.

3.2 The implementation of this Procedure will:

- Facilitate a fast response to incidents in order to contain or minimise the impact of the incident on data subjects affected by the incident, and minimise the university's exposure to legal and regulatory consequences, financial loss and reputational damage;
- Clarify the responsibilities of those involved in reporting data security incidents;
- Provide support to those who are affected by the incident, including the data subjects and those directly involved with the incident;
- Provide information regarding the causes of data security breaches so that improvements can be made to mitigate the risk of a further occurrence.
- Reporting incidents should be viewed positively and is to be encouraged, as they often result in improving knowledge of staff and improvement in procedures, as well as reducing risk and the impact on data subjects.

4.0 Definitions

4.1 Personal data: is defined in Article 4 as any information (for example, a person's name) or combination of information about a living person which allows that living person to be identified from that information (for example a first name and an address). Personal Data 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 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 GDPR as personal use of data is not governed by the GDPR.

5.3 The incident owner will normally be the Data Protection Officer or Service Delivery Manager and has primary responsibility for directing the investigation of the incident and ensuring that steps are taken to address the incident. The incident owner must not be the same as the individual who experienced/discovered the data loss.

5.4 It may be appropriate for a small team of experts to be called together to advise and deal with an incident. The composition of the team will very much depend on the nature of the data breach, but they may be from different departments including IS, legal, finance and marketing.

5.5 The Responsible Staff Member is the person who has primary day to day responsibility for the data which has been lost, and may also be the person who experienced or discovered the loss. The Responsible Staff Member plays an important role in providing information about the data which has been lost.

5.6 The IT Service Desk should ensure that incidents which are reported to them are reported to the Data Protection Officer or Legal Department and where necessary, to the Chief Technical Officer including an assessment of actual or potential security risks arising from an incident involving IT systems or equipment. This could include lost or stolen IT equipment or devices, or unauthorised access to data or systems.

6.0 Reporting and minimising data loss

6.1 It is important that incidents are reported through the correct channels as a matter of urgency, in order that the seriousness of the incident can be determined and so that advice can be provided on any immediate containment action required to minimise harm and data exposure. If an incident occurs or is discovered outside of normal working hours, it must be reported as soon as is practicable.

6.2 All staff have a responsibility to report incidents or suspected incidents under this procedure.

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.

7.2 The department concerned must co-operate promptly with the Data Protection Officer and Service Delivery Manager to avoid any delays. This includes completing the Incident Report form shown at Appendix 1 as quickly as possible following initial notification.

7.3 Not all data breach incidents will require reporting to the ICO. The decision whether to report the incident to the ICO will depend on the severity of the breach and will be based upon the assessment at Appendix 1. Any notification to the ICO will be in accordance with Para 9.3 below.

7.4 If it is concluded that a breach has occurred, depending upon the seriousness and complexity of the incident, it may be appropriate to draw together a team of experts who may all be able to offer expertise in their particular field.

7.5 The Director of Finance and the Procurement and Insurance Coordinator should also be informed at an early stage, as it may be necessary to take steps in order to comply with University insurance policies.

8.0 Confidentiality

8.1 From the time that a breach or loss is discovered, it is important that the incident remains confidential and that only those staff who need to, know about the incident. This will prevent rumours or incorrect information being released, which may cause distress to data subjects. Confidentially will enable effective steps to be taken to mitigate the incident.

8.2 To provide some privacy when reports and forms are circulated to the investigation team, individual data subjects must not be explicitly named in the reports or correspondence.

9.0 Actions and notifications

9.1 Any further actions to be taken will be determined following the investigation.

9.2 The communication of any data security breach to affected data subjects must be handled with care and sensitivity and appropriate advice will be provided.

9.3 Wider communication of a breach, including notification to any regulatory authorities, such as the Information Commissioner's Office, will be managed by the University Secretary, University Legal Advisor or the Data Protection Officer, or a staff member nominated by the Vice Chancellor or Deputy Vice Chancellor.

10.0 **Incident evaluation and follow up**

10.1 The incident may highlight remedial action which is required in relation to procedures, additional training requirements, IT systems or the incident reporting procedure. Any agreed actions and target dates for completion will be recorded on the Incident Report Form.

10.2 The Data Protection Officer will ensure that the Incident Report Form is completed and:

- Liaise with the relevant Incident Owner to ensure that local actions are completed,
- Escalate any actions which have not been completed by the target date,
- Ensure that guidance material is revised to reflect any learning outcomes,
- Report all data security breaches to the University Secretary for monitoring and oversight, and
- Propose improvement plan and actions where appropriate.

10.3 The University Secretary may recommend the instigation of the relevant disciplinary procedure for staff or misconduct procedure for students where the circumstances of a particular incident under this procedure make it appropriate to do so. The University Secretary will determine whether a referral to Human Resources is warranted.

10.4 This Procedure reflects the ICO Guidance on Data Security Breach Management which should be referred to for any queries. This Procedure will be reviewed at least every three years or when there are significant changes.

11.0 Examples of incidents that should be reported

IF UNSURE, REPORT IT

Use the Incident Report Form for incidents involving:

- 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,
- 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.

Appendix 1

Data breach or loss report form. **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	
Reported by *[Name, job title]*	
Has the line manager been informed? *(Not necessary if person is a manager)*	
Department	
Telephone	

1. Description of data lost, stolen or disclosed *[include examples of type of data, volumes of records affected and number of data subjects involved. Where relevant specify device make, model and serial number. Where a mobile device has been lost or stolen, please include name of the person who lost it]*
If a misdirected email, please forward a copy to the service desk & see No 6 below.
2. Circumstances of the loss, theft or disclosure *[include timing of events; location; IT media and applications involved; details of actions taken to date, e.g., anyone who has been contacted in relation to the incident]*
3. Details of any other regulatory body or collaborative partner who may need to be informed *[e.g. HEFCE, BASIS, research partner etc.]*

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 ☐ No ☐
- Can an email be deleted from the inbox of the incorrect recipients? Yes ☐ No ☐
- 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 ☐ No ☐
- Is it possible to remotely delete or wipe the lost article? Yes ☐ No ☐

7. Any other information, factors or views that investigators should be aware of?

8. Have you informed your line manager about the data breach?
(If appropriate – will depend on who is reporting the incident)

For completion by DPO

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 ☐ No ☐ Completed ☐ **Do the data subject(s) need to be informed?** **Yes ☐ No ☐ Completed ☐**
11. Details of investigation by DPO
12. Learning outcomes of the investigation
13. Incident closed with Service Desk?
Yes ☐ No ☐