University of HUDDERSFIELD
Inspiring tomorrow's professionals

DATA PROTECTION POLICY

Contents

DATA PROTECTION POLICY

Purpose and Context

The University of Huddersfield is committed to a policy of protecting individuals' right to privacy in accordance with the Data Protection Act 1998 (including any replacement of that Act) (the "**DPA**") and the General Data Protection Regulation (the "**GDPR**", together, the "**Data Protection Laws**"). This policy sets out that commitment. The University recognises that correct and lawful treatment of Personal Data contributes to the good reputation of the University by demonstrating its integrity and its respect for those it deals with. The University needs to Process certain information about its staff, students and other individuals it has dealings with. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Scope

This policy encompasses all Processing of Personal Data by staff, students and affiliates, each of whom are subject to this policy. As a matter of good practice, other organisations or agents who have access to and Process Personal Data on behalf of the University will be expected to have read and comply with this policy. It is the responsibility of the relevant School or Service who deal with such external third parties to ensure that such third parties agree in writing to abide by this policy, with support from published procedures and guidance, and from the University Data Protection Officer.

1. Policy Statement

1.1 This policy does not form part of the formal contract of employment for staff, but it is a condition of employment that employees will familiarise themselves with and act in accordance with this policy. The University may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be managed in accordance with the University's policy framework.

1.2 Any failure to follow this policy by staff or students may result in disciplinary action. Any failure by affiliates to follow this policy may result in their access to University IT systems and premises being restricted or removed.

2. Background

2.1 The purpose of the Data Protection Laws is to protect the rights and privacy of living individuals and to ensure that Personal Data is Processed fairly and transparently.

2.2 The University collects, holds and uses Personal Data relating to individuals who have/have had a relationship with the University. The purpose of this policy is to ensure that the University:

2.2.1 operates procedures and practices that conform to the requirements of the Data Protection Laws when working with Personal Data;

2.2.2 clearly defines responsibilities and accountability for data protection; and

2.2.3 provides staff, researchers and students with the resources, knowledge, competencies and procedures to work with Personal Data in compliance with the Data Protection Laws and with this policy.

2.3 Breach of the Data Protection Laws can lead to enforcement action by the Information Commissioner's Office, which can now impose monetary penalties on the University of up to €20,000,000. The University might also be sued by any individuals affected by the breach. In addition, individuals may also be subject to fines and criminal liability where they are found to have breached the Data Protection Laws.

3. Data Protection Definitions

This policy tries as far as possible to avoid using technical terms. However, there are some terms used in the Data Protection Laws that it is helpful to have an understanding of in the context of data protection compliance. To assist such understanding, we have set out a list of key terms and their meanings below. Where these terms are used in this policy, they should be read and applied in this context.

"**Data Subject**"	Any living individual who is the subject of Personal Data held by an organisation.
"**Data Controller**"	In the context of the majority of Personal Data held by the University, the University will be the Data Controller. A Data Controller is any person (or organisation) who makes decisions with regard to particular Personal Data, including decisions regarding the purposes for which Personal Data is Processed and the way in which the Personal Data is Processed.
"**Personal Data**"	Data relating to a living individual who can be identified from that information or from that data combined with other information in possession of the University. Includes name, address, telephone number, student or staff ID number, details of schools attended and photographs (which may also constitute Sensitive Personal Data). Also includes expression of opinion about the individual, and of the intentions of the University in respect of that individual.

"**Process or Processing**"	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"**Sensitive Personal Data**"	or "**Special Categories of Personal Data**" means Personal Data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data for the purpose of uniquely identify a person (e.g. fingerprints), data concerning physical or mental health or condition (e.g. substance abuse testing), sexual life, criminal offences, or related proceedings. Any use of Sensitive Personal Data or Special Category Data must be strictly controlled in accordance with this policy.
"**Third Party**"	Any individual/organisation other than the Data Subject or the Data Controller (i.e. the University) or an employee of the University who is Processing Personal Data on behalf of the University in accordance with this policy.

4. Responsibilities Under the Data Protection Laws

4.1 The University is the Data Controller in respect of Personal Data Processed by and for the University.

4.2 The senior post holder with overall responsibility for this policy is the University Secretary on behalf of the University Senior Management Team.

4.3 The University Secretary has delegated responsibility for day-to-day data protection matters to the University Solicitor, who has been appointed as the Data Protection Officer for the University.

4.4 The Data Protection Officer is Rebecca McCall and can be contacted at data.protection@hud.ac.uk.

4.5 An Information Governance Group (IGG) has been established to define, approve, steer and monitor Information Management (including in relation to data protection) within the University. This includes overseeing information governance roles and responsibilities, policies and procedures and activities in order to embed compliance, promote best practice, and provide technical solutions within all Schools and Services.

4.6 Deans, Directors and Heads of Service within the University have overall responsibility for the Processing of Personal Data within their own Schools or Services and for ensuring that such Processing is undertaken in a way that is compliant with this policy. All those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the University, but ultimately, compliance with data protection legislation is the responsibility of all members of the University who Process Personal Data.

4.7 Each School and Service has a designated Data Protection Champion who acts as a first point of contact for that School or Service relating to data protection issues. The Data Protection Champions raise awareness of data protection and information security responsibilities, policies and processes within the School/Service, and promote the maintenance and disposal of information held by the School/Service in accordance with University policies and procedures. The Data Protection Champions are supported by the University Data Protection Officer, and by the Information Security Manager, who provide them with guidance, information, updates and training.

4.8 All staff are responsible for:

4.8.1 ensuring that they have undertaken University-provided data protection training;

4.8.2 checking that any information that they provide the University in connection with their employment is accurate and up to date and for informing the University of any changes to their personal data (e.g. change of address); and

4.8.3 ensuring that any Personal Data Processed by them is Processed in accordance with the Data Protection Laws and with this policy.

4.9 Staff who have a responsibility for supervising/mentoring students who are undertaking Processing of Personal Data (e.g. as part of a research project or on a placement) have a responsibility to ensure that the student is informed as to their responsibilities under the Data Protection Laws, by reference to this policy and other relevant materials. For the avoidance of doubt, students on placement at the University should not be given access to ASIS.

4.10 All students are responsible for checking that any information that they provide the University in connection with their enrolment and study at the University is accurate and up to date and for informing the University of any changes to their Personal Data (e.g. change of address).

4.11 Students who are considering Processing Personal Data as part of their studies must notify and seek approval from their Head of Department as part of the relevant School's research ethics approvals process. Such students will be bound by the Data Protection Laws and by this policy and must ensure that they act in accordance with both.

5. Data Protection Principles

5.1 The University's policy is to Process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All staff have personal responsibility for the practical application of the University's data protection policy.

5.2 The University will observe the principles set out in the Data Protection Laws in respect of the Processing of Personal Data and will adhere to the following principles:

5.2.1 to Process lawfully, fairly and transparently. Those responsible for Processing Personal Data (see section 4 above) must make reasonable efforts to ensure that Data Subjects are informed of the identity of the Data Controller (i.e. the University), the purpose(s) and legal basis of the Processing, any disclosures to third parties that are envisaged and an indication of the period for which the Personal Data will be kept.

5.2.2 to obtain personal data for specific, explicit and legitimate purposes. Personal Data will not be Processed in a manner incompatible with those purposes, and Personal Data obtained for specified purposes must not be used for a different purpose.

5.2.3 to ensure that the Personal Data is adequate, relevant and not excessive in relation to the purposes for which it is used. Information that is not strictly necessary for the purpose for which it is obtained should not be collected. If Personal Data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

5.2.4 to keep Personal Data accurate and up to date (and where inaccurate ensure they are erased and rectified without delay). Personal Data that is kept for a long time must be reviewed and updated as necessary. No Personal Data should be kept unless it is reasonable to assume that it is accurate.

It is the responsibility of all individual staff, students and other persons to ensure that Personal Data held by the University is accurate and up to date. Completion by a Data Subject of an appropriate registration or application form, etc. will be taken as an indication that the data contained therein is accurate. Individuals should notify the University of any changes in circumstance to enable personal records to be updated accordingly. Students should use "My Details" or contact the Student Records Team (applicants should contact the Student Recruitment Team). Staff should contact their Human Resources representative in Human Resources or update their personal details using My HR. It is the responsibility of the University to ensure that any notification regarding change of circumstances is noted and acted upon.

5.2.5 not to be keep Personal Data for longer than is necessary for the purposes for which it is used (see Section 14 on Retention and Disposal of Data); and

5.2.6 to keep Personal Data secure to prevent unauthorised or unlawful Processing and accidental loss, damage or destruction, using appropriate technical or organisation measures. (see Section 8 on Security of Data).

5.2.7 to Process Personal Data in accordance with the rights of data subjects in accordance with the Data Protection Laws (see Section 6 on Data Subject Rights).

5.2.8 not to transfer Personal Data to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the Processing of Personal Data (see Section 15 on International Transfers).

5.3 The University should generally not Process Personal Data unless:

5.3.1 it is to fulfil a contract with the individual (be this a student, a member of staff or a third party); or

5.3.2 the Processing is necessary to comply with the University's legal obligations or exercise legal rights; or

5.3.3 the Processing is required for a task in the public interest, or in the exercise of the University's official authority

5.3.4 the Processing is in the University's legitimate interests and does not unduly prejudice the individual's privacy.

5.4 To the extent the University Processes Special Categories of Personal Data, it must ensure that such Processing satisfies the conditions for Processing required by the Data Protection Laws (see Section 7 on Special Categories of Personal Data).

5.5 Transparency is key to data protection. Individuals should be told how, why and on what basis their personal data is being Processed.

5.6 The University will publish privacy notices in respect of its Processing of Personal Data of students, staff, alumni, certain partners and visitors, which tell those people what data is collected about them, what it is used for, the legal basis for Processing the data, who it will be shared with and how long it will be held for. When gathering Personal Data or establishing new data protection activities, members of staff should check existing privacy notices to see whether they need to be updated to reflect the new activities, or whether new privacy notices are required to cover that activity. There are limited exceptions to this notice requirement. In any case of uncertainty as to whether a notification should be given or updated, staff should contact their Data Protection Champion. In the event that staff or students Process Personal Data on behalf of another party (as a part of research activities or otherwise), due diligence should be carried out (and contractual protection obtained) to ensure appropriate data protection notices or consents have been given or obtained.

6. Data Subject Rights

6.1 Under the Data Protection Laws, Data Subjects have the following rights regarding the Processing of their Personal Data and the data that are recorded about them:

6.1.1 to access personal data held by the University about them (please see Section 12); to require the University to rectify any inaccurate personal data held by it about them; and to require the University to erase personal data held by it about them. This right of erasure will only apply where, for example, the University no longer needs to use the Personal Data to achieve the purpose it collected it for; or where the Data Subject withdraws their consent if the University is using their Personal Data based on Data Subject consent; or where the Data Subject objects to the way the University Processes their data and this is upheld;

6.1.2 to restrict the University's Processing of the Personal Data it holds about them. This right will only apply where, for example, the Data Subject disputes the accuracy of the Personal Data the University holds; or where they would have the right to require the University to erase the Personal Data but would prefer that its Processing is restricted instead; or where the University no longer needs to use the Personal Data to achieve the purpose for which it was collected, but it requires the data for the purposes of dealing with legal claims. In cases where the University has disclosed data to another party, and it is not disproportionate for the University to do so, it will let the recipients of the data know that the University has rectified, erased or restricted its Processing of it;

6.1.3 to receive personal data, which they have provided to the University, in a structured, commonly used and machine readable format (where Processing is automated and is either based on consent or is necessary for the performance of a contract). Data Subjects also have the right to transfer (or require the University to transfer) this Personal Data to another organisation (for example, a new employer or higher education institution);

6.1.4 to object to the University's Processing of Personal Data it holds about them (where its justification for Processing the data is either that the Processing is necessary for the performance of a task in the public interest, or for the purposes of its own legitimate interests);

8.1.5 to require a review. Data Subjects may ask the University to review any decisions that it has made about them using automated Processing;

6.1.6 to withdraw their consent, where the University is relying on it to Process their personal data.

6.1.7 to prevent Processing for the purposes of direct marketing;

6.2 The University will have procedures in place to ensure that these rights can be exercised and will publicise these on its website.

6.3 If staff or students have concerns about the way in which their personal data is being used or Processed by the University, they may contact a Data Protection Champion or the Data Protection Officer, in the first instance. If after this, they are not satisfied by the University's response they have the right to lodge a formal complaint with the Information Commissioner's Office.

7. Special Categories of Personal Data

7.1 Special Categories of Personal Data are afforded a higher level of protection by law. It will normally be necessary to have an individual's explicit consent to Process Special Categories of Personal Data, unless exceptional circumstances apply or the Processing is necessary to comply with a legal requirement, including to fulfil employment duties as an employer. The consent should be a freely given (i.e. it should not be conditional), specific (i.e. it should set out exactly what is being consented to), informed, (i.e. it needs to identify the relevant data, why it is being Processed and to whom it will be disclosed) and an unambiguous indication of the individual's wishes by which they, by a statement or by a clear affirmative action (i.e. the ticking of an unticked box) signify their agreement. Staff should contact the Data Protection Officer for more information about the conditions to be satisfied to enable Processing of Special Category Personal Data.

7.2 The University will not rely on consent for the purposes of Processing staff Personal Data save in limited circumstances where it can be demonstrated that there is a genuine choice and the consent was freely given. If any member of the University wishes to Process any Personal Data by relying on consent as a means to do so they must consult the Data Protection Officer for further guidance.

8. Security of Data

8.1 All staff are responsible for ensuring that any Personal Data (on others) which they hold are kept securely in line with the University's IT Security Policy and Procedure and that such data is not disclosed to any unauthorised third party (see Section 13 on Disclosure of Data for more detail).

8.2 All Personal Data should be accessible only to those who need to use it. A judgment should be made based upon the sensitivity and value of the information in question, but consideration should always be given to keeping Personal Data:

8.2.1 in a lockable room with controlled access;

8.2.2 in a locked drawer or filing cabinet; or

8.2.3 if computerised, password protected.

8.3 Personal Data must not be stored on removable media (such as USB storage devices, removable hard drives, CDs or DVDs) or mobile devices (laptops, tablets or smart phones) unless it is encrypted or password protected, and the key kept securely. A backup copy should also be kept on the secure University servers. Personal Data must not be stored in generic personal cloud services such as Dropbox.

8.4 Care should be taken when sending emails that contain Personal Data. Further guidance on the use of email is available from the University Records Management pages.

8.5 If Personal Data is transferred using removable media, a secure, tracked service must be used to ensure safe delivery.

8.6 Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised individuals.

8.7 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of Personal Data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be securely wiped clean before disposal. If in doubt as to what the correct security measures are for the deletion or disposal of Personal Data, advice should be taken from IT Support or the University Records Manager, as appropriate.

8.8 This policy also applies to staff and students who Process Personal Data "off-site". Off-site Processing presents a potentially greater risk of loss, theft or damage to Personal Data. Staff and students should take particular care when Processing Personal Data at home or in other locations outside the University campus and should comply with the University's Regulations governing use of Computing Facilities and with the IT Security Policy and Procedures.

8.9 Where the University uses external organisations to Process Personal Data on its behalf additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of Personal Data. There are also mandatory legal protections which must be included in any contract with such parties.

8.10 In the event that the University acts as a Data Processor (please see below), Processing personal data on behalf of a third party, such third party may require additional security arrangements to be implemented. There are also mandatory legal protections with must be included in any contract, which needs to be flowed-down to any sub-processor used by the University.

8.11 Members of the University should consult their line manager or the Data Protection Officer to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

9. Reporting Breaches

9.1 Members of the University have an obligation to report actual or potential data protection compliance failures to the Data Protection Officer immediately they become aware of them, following the published breach notification procedure. The Data Protection Laws provide that breaches must be notified to the ICO as soon as possible and in any event within 72 hours of becoming aware of them. Notification to the Data Protection Officer also allows the University to:

9.1.1 investigate the failure and take remedial steps if necessary; and

9.1.2 make any other applicable notifications, including to affected Data Subjects where appropriate.

9.2 University staff may be requested as part of their duties to support the University in any such investigation.

9.3 Where the University is acting as a Data Processor, it will have a responsibility to notify actual or potential data protection compliance failures to the third party it is Processing personal data on behalf of. The contract between the University and the third party it is Processing personal data on behalf of may also have additional contractual restrictions or timescales in respect of such support/ assistance. Members of the University should check the contractual position carefully and check with the Data Protection Officer if they are unclear how to proceed.

10. Acting as a Data Processor

10.1 When the University Processes the Personal data of students, staff, suppliers, alumni, and other individuals (in a professional or personal context) it is ordinarily the case that the University would be known as a Data Controller. A Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, Processed.

10.2 In some limited circumstances, the University may be a Data Processor; i.e. it is Processing the data on behalf of a third party Data Controller.

10.3 If Members of the University are handling Personal Data and are not sure whether the University is acting as a Data Controller or a Data Processor, they should contact their line manager, Data Protection Champion or Data Protection Officer in the first instance. It is key to understand the relationship, in order to determine how such personal information should be handled.

10.4 The Data Controller has the majority of the obligations under the Data Protection Laws, e.g. in respect of Data Subject rights and ensuring appropriate consents are obtained or privacy notices are given. However, a Data Processor also has a number of obligations under Data Protection Laws. In most cases, the Processing obligations imposed on the University will be guided by the contract entered into between the University and the third party on whose behalf it is Processing.

11. Accuracy, Adequacy, Relevance and Proportionality

11.1 Members of the University should make sure data Processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal Data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

11.2 Individuals may ask the University to correct Personal Data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does

not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the Data Protection Officer.

11.3 Staff and students must ensure that Personal Data held by the University relating to them is accurate and updated as required. If personal details or circumstances change, staff and students should inform Human Resources (including via MyHR) or the Student Records Office (or online via My Details) respectively so the University's records can be updated.

12. Rights of Access to Personal Data

12.1 As set out above, individuals have the right (subject to certain exceptions) to request access in relation to information held by the University about them in electronic format and/or in manual records which form part of a relevant filing system, save where exemptions apply. A request of this nature is known as a "subject access request". All such requests should be referred immediately to the Data Protection Officer. This is particularly important because the University must respond to a valid request within the legally prescribed time limits.

12.2 Any individual who wishes to exercise this right should apply in writing to the University Data Protection Officer. The University must respond to requests without delay and in any event within one month of their receipt. In order to assist the University Data Protection Officer in complying with such requests, it is helpful if the form provided through the University's Data Protection webpages is completed. For information on responding to subject access requests in accordance with the Data Protection Laws see the guidance available on the Information Governance website.

12.3 Where a request is made for examination scripts (where these are still held), no copies of the scripts will be provided but students may view the script in the presence of a representative from Registry. Examiners' comments can be transcribed and provided as part of a subject access request.

12.4 In order to respond efficiently to data subject rights requests the University needs to have in place appropriate records management practices. See the University Records Management pages for further information on records management.

12.5 In addition to the above, where the University is acting as a Data Processor, it will have a responsibility to provide assistance to the third party it is Processing Personal Data on behalf of, in respect of individuals exercising their rights. The contract between the University and the third party it is Processing Personal Data on behalf of, may also have additional contractual restrictions or timescales in respect of such support/ assistance. You should check the contractual position carefully prior to (a) responding to a request made directly by an individual, third party or the ICO, or (b) providing assistance to the third party; and check with the Data Protection Officer if you are unclear how to proceed.

13. Disclosure of Personal Data

13.1 The University must ensure that Personal Data is not disclosed to unauthorised third parties. This includes family members, friends, government bodies, the media, and in certain circumstances, the Police.

13.2 All staff and students should exercise caution when asked to disclose Personal Data held by the University about another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's personal details to someone who wished to contact them regarding a non-work related matter, especially when such details are not otherwise publicly available (such as work contact details on the University website). The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of University business.

13.3 This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

13.3.1 where the disclosure is in the legitimate interests of the University (e.g. disclosure to staff – Personal Data can be disclosed to other University employees if it is clear that those members of staff require the information to enable them to perform their jobs);

13.3.2 where the University is legally obliged to disclose the data (e.g. HESA and HESES returns, ethnic minority and disability monitoring, all of which are covered in the University's privacy notices for staff and students); or

13.3.3 where disclosure of data is required for the performance of a contract (e.g. informing Student Finance England or a sponsor of course changes/withdrawal, etc.).

13.4 If Personal Data is to be shared with a third party in connection with the performance of a contract, then approved data protection clauses must be included in the relevant contract. The University Data Protection Officer should be consulted on every occasion before any such contracts are entered into and Personal Data must not be shared with the third party until an appropriate contract is in place.

13.5 The Data Protection Laws permit certain disclosures without notification to the Data Subject in certain cases, so long as the information is requested for one or more of the following purposes:

13.5.1 to safeguard national security[1]**;

13.5.2 prevention or detection of crime including the apprehension or prosecution of offenders**;

13.5.3 assessment or collection of tax duty**;

13.5.4 discharge of regulatory functions (includes health, safety and welfare of persons at work)**;

13.5.5 to prevent serious harm to a third party; or

13.5.6 to protect the vital interests of the individual; this refers to life and death situations.

** Requests must be supported by appropriate paperwork and should follow the agreed protocols. Where no formally agreed protocol is in place, or if members of the University are in any doubt as to whether or not it is appropriate that a disclosure is made, they should contact the University Data Protection Officer.

13.6 When members of staff receive enquiries as to whether a named individual is a member of the University (staff or student), the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the University may constitute an unauthorised disclosure of Personal Data.

13.7 Unless the Data Subject has requested otherwise, Personal Data should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the Data Subject consenting to disclosure to the third party should accompany the request.

13.8 As an alternative to disclosing Personal Data, the University may offer to do one of the following:

13.8.1 pass a message to the Data Subject asking them to contact the enquirer; or

13.8.2 accept a sealed envelope/incoming email message and attempt to forward it to the Data Subject.

13.9 Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the University" to avoid confirming their membership of, their presence in or their absence from the institution.

13.10 Further information regarding the disclosure of personal information can be found in the guidance available on the Information Governance website.

13.11 If in doubt, staff should seek advice from their line manager or Data Protection Champion within their School or Service, or the University Data Protection Officer.

14. Retention and Disposal of Data

14.1 The University discourages the retention of Personal Data for longer than it is required. Considerable amounts of data are collected about staff, students, applicants, research subjects, etc. However, once a member of staff or student has left the University or the purpose for which that data was collected has ended, it will

not be necessary to retain all the information held on them. Some Personal Data will be kept for longer periods than others. The University's Retention and Disposal Schedule should be followed for the retention and disposal of Personal Data.

14.2 The University aims to reduce the duplication of personal data and will encourage as far as possible the use of definitive central sources of information for data used across the University (e.g. contact addresses). Those with legitimate reason will have access to the Personal Data relevant for their job. Permissions granted for such access will be logged where possible and regularly reviewed.

14.3 The creation of systems and/or files which duplicate such data should be avoided; where it is inevitable every care should be taken to ensure that data maintained in subsidiary systems is fully synchronised with definitive sources, and updated frequently through secure and reliable interconnection.

Students

14.4 In general, electronic student records maintained in the University's Applicant and Student Information System (ASIS) are kept permanently in order to fulfil the requirement for the provision of transcripts during a student's or former student's working life. Such information would typically include name and address on entry and completion, programmes taken, examination results and awards obtained.

14.5 Schools and Services should regularly review the personal files that they hold relating to individual students (whether stored electronically or in paper records) in accordance with the University's Retention and Disposal Schedule.

Staff

14.6 In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by Human Resources for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay, etc. will be retained for the statutory time period (between 3 and 6 years).

14.7 Staff Human Resources records are kept and maintained by Human Resources. Other departments should only keep staff information where necessary for legitimate business purposes. To the extent that files of individual staff members are kept outside Human Resources, departments should regularly review those files of in accordance with the University's Retention and Disposal Schedule.

14.8 Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for six months from the interview date and should then be securely destroyed as confidential waste. Human Resources may keep a record of names of individuals that have applied, been short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

Disposal of Records

14.9 Personal Data must be disposed of in a way that protects the rights and privacy of Data Subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion) and in line with the University's Retention and Disposal Schedule.

15. International Transfers

15.1 Data must not be transferred outside of the European Economic Area (EEA) - the twenty-eight EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual, or unless the Personal Data is adequately protected or an exemption applies.

15.2 Adequate protection can be provided if:

15.2.1 the data protection arrangements in the destination country have been approved by the EU Commission (there is a list of approved countries on the EU commission website); or

15.2.2 the recipient is a signatory to an EU approved data protection regime; or

15.2.3 the recipient is bound by a contract that ensures that the Personal Data concerned will be adequately protected (for example, using the standard form agreement approved by the EU for this purpose).

15.3 Members of the University should be particularly aware of this when contracting with a third party for the Processing of Personal Data (including for IT support, collaborative provision, or research purposes) or when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

15.4 In addition to the above, where the University is acting as a Data Processor, the contract between it and the third party it is Processing Personal Data on behalf of may have additional contractual restrictions in respect of international transfers of such data. Members of the University should check the contractual position carefully prior to transferring the Personal Data and check with the Data Protection Officer if they are unclear how to proceed.

16. Publication of University Information

16.1 The University publishes a number of items that include Personal Data, and will continue to do so. These are:

16.1.1 names of all members of University Committees (including Council and Senate);

16.1.2 academic staff profiles on the University website, including names, job titles and academic and/or professional qualifications and photographs;

16.1.3 Awards and Honours (including Honorary Graduands and other Honorary award recipients, Emeritus Professors and Prize-winners);

16.1.4 Staff Telephone and Email Directory;

16.1.5 graduation programmes and videos or other multimedia versions of graduation ceremonies;

16.1.6 information in prospectuses (including photographs), annual reports, staff newsletters, etc.;

16.1.7 publicity information included in public relations stories and press releases and on social media; and

16.1.8 staff information on the University website (including photographs).

16.2 It is recognised that there might be occasions when a member of staff, a student, or other party, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the University should use its reasonable endeavours to comply with the request and ensure that appropriate action is taken.

17. Direct Marketing

17.1 Any proposal to carry out direct marketing (i.e. marketing by email, telephone, post or any other means that is directed at a particular individual, whether they are a student, applicant, alumnus, member of staff or otherwise) must be reviewed and approved in advance by the University Data Protection Officer in conjunction with the Central Marketing team.

17.2 Members of the University should not send direct marketing material to someone electronically (e.g. by email, Whatsapp, social media messenger services or targeted banner ads) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their Personal Data for direct marketing purposes and should notify the relevant marketing team about any such request.

17.3 Any School or Service that uses Personal Data for direct marketing purposes must inform Data Subjects of this at the time of collection of the relevant Personal Data and may only make direct marketing communications where the Data Subject has opted-in to receiving such communications. Data Subjects must also be given the opportunity to opt out of receiving communications at any time and measures must be put in place to prevent such communications from being sent once the University has received confirmation that a Data Subject has opted out.

18. Use of CCTV

18.1 The University's use of CCTV is regulated by a separate Code of Practice.

18.2 For reasons of personal security and to protect University premises and the property of staff and students, close circuit television cameras are in operation in certain campus locations. This policy determines that personal data obtained during monitoring will be processed as follows:

18.2.1 any monitoring will be carried out only by a limited number of specified staff;

18.2.2 the recordings will be accessed only by the Security Manager, Senior Management and staff authorised by the Security Manager or Senior Management;

18.2.3 personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete in line with the University's Retention and Disposal Schedule; and

18.2.4 staff involved in monitoring will maintain confidentiality in respect of Personal Data.

19. Academic Research

19.1 Personal Data collected only for the purposes of academic research (includes work of staff and students) must be Processed in compliance with the Data Protection Laws and in compliance with the University's Research Data Management Policy and its Research Ethics and Integrity Policy and procedures. The University will publish additional guidance to assist researchers in complying with these requirements.

19.2 Individual students or staff carrying out research should note that Personal Data may be Processed for research purposes on the legal basis that the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the University. Researchers may also rely on the bases that the Processing is necessary for scientific or historical research purposes, or that it is necessary for statistical purposes.

19.3 Where the legal bases for Processing Personal Data referred to above are available to researchers, the consent of the Data Subject is not required. However, such Processing is subject to safeguards to ensure that data is minimised (including being pseudonymised, and if possible anonymised) and that:

19.3.1 the Personal Data are not Processed to support measures or decisions with respect to particular individuals; and

19.3.2 the Data Subjects must not be caused substantial damage or substantial distress by the Processing of the Personal Data.

19.4 If the above conditions are met, together with technical and organisational safeguards to keep data secure, Personal Data Processed for research purposes may be:

19.4.1 Processed for purposes other than that for which it was originally obtained, including statistical or historical purposes; and

19.4.2 exempt from the Data Subject's right of access and rectification, as well as their right to restrict or object to Processing.

19.5 Other than this, Data Protection Laws apply in full in respect of academic research. The obligations to collect only necessary and accurate Personal Data, to hold Personal Data securely and confidentially and not to disclose Personal Data except

in accordance with the Data Protection Laws (including in relation to publication) must all still be complied with.

Publication

191.9 Researchers should ensure that the results of research are anonymised when published and that no information is published that would allow individuals to be identified (including where anonymised data could be matched with other data to link back to an identifiable individual) where consent has not been obtained for such use from the Data Subject or, where the nature of the research makes it impracticable or otherwise undesirable to attempt to seek/obtain consent, that there is a legitimate interest in publication and publication would not unfairly damage the rights and freedoms of the Data Subject.

20. Data Protection Impact Assessment

20.1 To help the University meet its data protection obligations and to meet staff and students' expectations of privacy, the University carries out Privacy Impact Assessments ("PIA"s) prior to beginning any new Processing activities. Although these are only required under Data Protection Laws for the large scale Processing of Sensitive Personal Data, systematic monitoring of a public area on a large scale, the systematic evaluation of individuals based on automated Processing, and other Processing activities which are likely to result in a high risk to the rights of Data Subjects, it is good practice to carry out PIAs when embarking on new projects involving the Processing of Personal Data.

20.2 The data protection regulator in the UK also requires PIAs to be carried out where an organisation plans a number of specific Processing activities, including using new technology, Processing biometric data, collecting Personal Data from a source other than the Data Subject without providing them with a privacy notice. The PIA is a method by which the University can assess and address the risk its Processing of Personal Data will present, and is consistent with 'Privacy by Design' - an approach by which data protection is built into a project from the outset, and not bolted on at the end.

20.3 The PIA involves setting out the envisaged Processing, its purposes, and the legal basis under which it is to be processed. It involves an assessment of the risks posed by the Processing to the rights and freedoms of the Data Subjects, and the measures to be taken to address those risks. It will include an analysis of safeguards being put in place, and will demonstrate how the Processing will be compliant with the Data Protection Laws. Once the University has carried out a PIA, it will keep it under regular review to ensure that the assessment of risk addresses circumstances as they change.

20.4 The PIA process is managed by the University Records Management team and more information is available via the Records Management webpages.

21. Further Information

21.1 Useful web addresses:

- University Information Governance pages
- Information Commissioner's Office
- HESA privacy information

21.2 For further guidance or advice on the Data Protection Laws or this policy and its application, please contact the University Data Protection Officer by email at data.protection@hud.ac.uk.

Additional Guidance

23.3 The University has published a number of guidance notes relating to data protection compliance, all of which are available on the University's Information Governance website.

POLICY SIGN-OFF AND OWNERSHIP DETAILS	
Document name:	Data Protection Policy
Version Number:	1.0
Equality Impact Assessment:	To follow
Approved by:	SMT
Date Approved:	26 April 2018
Next Review required by:	26 April 2021
Author:	University Data Protection Officer
Owner (if different from above):	University Secretary
Document Location:	https://www.hud.ac.uk/media/policydocuments/Data-Protection-Policy.pdf
Compliance Checks:	Data breach audit/follow-up, monitor training, feedback from Data Protection Champions.
Related Policies/Procedures:	Records Management Policy Retention Schedules IT Security Policy IT Security Procedures Information Security pages Research Data Management Policy Research Ethics and Integrity Policy

REVISION HISTORY			
Version	**Date**	**Revision description/Summary of changes**	**Author**
1.0	26 April 2018	Major redraft – first version under Policy Framework. Previous versions available from University Secretary's Office	University Solicitor