University of HUDDERSFIELD

Data Protection Policy

Contents

Version:	2.1 (25.06.15)
Policy Owner(s):	University Secretary's Office
Policy Approved by/Date:	SMT/25.06.15
Date of Review	25.06.18

University of HUDDERSFIELD

1. Policy Statement

1.1 The University of Huddersfield is committed to a policy of protecting individuals' right to privacy in accordance with the Data Protection Act 1998 (the **DPA**). 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.

1.2 This policy encompasses all processing of Personal Data by staff and students, 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 the University Data Protection Officer.

1.3 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.

1.4 Any failure to follow this policy by staff or students may result in disciplinary action.

2. Background to the Data Protection Act 1998

The purpose of the DPA is to protect the rights and privacy of living individuals and to ensure that Personal Data is not processed without their knowledge, and, wherever possible, is processed with their consent.

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:

2.1 operates procedures and practices that conform to the requirements of the DPA when working with Personal Data;

2.2 clearly defines responsibilities and accountability for data protection; and

2.3 provides staff, researchers and students with the resources, knowledge, competences and procedures to work with Personal Data in compliance with the DPA and with this policy.

Breach of the DPA can lead to enforcement action by the Information Commissioner's Office, which can impose monetary penalties on the University of up to £500,000. The University might also be sued by an individual affected by the breach. In addition, individuals may also be subject to fines and criminal liability where they are found to have breached the DPA without the University's consent.

3. DPA Definitions

This policy tries as far as possible to avoid using technical terms. However, there are some terms used in the DPA 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:	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. In the context of the majority of Personal Data held by the University, the University will be the Data Controller.
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 related to the collection, obtaining, recording, holding and storing of Personal Data and carrying out any operations on it, including adaptation, alteration, use, disclosure, transfer, erasure and destruction.
Sensitive Personal Data:	This is a sub-category of Personal Data and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive Personal Data is subject to much stricter conditions of processing.
Third Party:	Any individual/organisation other than the Data Subject or the Data Controller (i.e. the University).

4. Responsibilities under the Data Protection Act

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 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.

4.5 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.

4.6 Each School and Service must have a designated data protection contact who acts as a first point of contact for that School or Service relating to data protection issues. The Deans, Directors and Heads of Service are responsible for ensuring that the details of the relevant points of contact are provided to the University Data Protection Officer and are kept up to date. The University Data Protection Officer, supported by the IGG, is responsible for liaising with these local contacts, for providing guidance, support and training and for monitoring of standards.

4.7 All **staff** are responsible for:

4.7.1 ensuring that they have undertaken University provided data protection training;

4.7.2 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

4.7.3 ensuring that any Personal Data processed by them is processed in accordance with the DPA and with this policy.

4.8 **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 DPA, by reference to this policy and other relevant materials.

4.9 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).

4.10 **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 DPA and by this policy and must ensure that they act in accordance with both.

5. Notification

5.1 The DPA requires every organisation that processes personal information to register with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence.

5.2 Notification is the responsibility of the University Secretary and the University Data Protection Officer. Details of the University's notification, including a description of the kind of processing of Personal Data carried out by the University are published on the Information Commissioner's Office website. The University's registration number is Z6534300 and the notification is reviewed annually.

5.3 Anyone who processes, or intends to process, Personal Data for purposes not included in the University's current notification should seek advice from the University Data Protection Officer.

6. Data Protection Principles

6.1 All processing of Personal Data must be done in accordance with the eight data protection principles:

1	**Personal Data shall be processed fairly and lawfully.** 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) 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.
2	**Personal Data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.** Personal Data obtained for specified purposes must not be used for a purpose that differs from those.
3	**Personal Data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.** 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.
4	**Personal Data shall be accurate and, where necessary, kept up to date.** 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 Admissions and Records Office. Staff should contact their personnel 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	**Personal data shall be kept only for as long as necessary.** (see Section 12 on Retention and Disposal of Data)
6	**Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.** (see Section 7 on Data Subject Rights)
7	**Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.** (see Section 9 on Security of Data).

8	**Personal data shall not be transferred 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.** Data must not be transferred outside of the European Economic Area (**EEA**) - the fifteen EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. 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.

7. Data Subject Rights

7.1 Data Subjects have the following rights regarding the processing of their Personal Data and the data that are recorded about them:

7.1.1 to know what information the University holds and uses about them and why;

7.1.2 to make subject access requests regarding the nature of information held and to whom it has been disclosed (see Section 10);

7.1.3 to prevent processing likely to cause unwarranted damage or distress;

7.1.4 to prevent processing for purposes of direct marketing;

7.1.5 to be informed about mechanics of automated decision-taking process that will significantly affect them;

7.1.6 not to have significant decisions that will affect them taken solely by automated process;

7.1.7 to sue for compensation if they suffer damage by any contravention of the Act;

7.1.8 to take action to rectify, block, erase or destroy inaccurate data; and

7.1.9 to request the Information Commissioner's Office to assess whether any provision of the Act has been contravened.

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

8. Consent

8.1 Wherever possible Personal Data or Sensitive Personal Data should not be obtained, held, used or disclosed unless the individual has given consent. For Sensitive Personal Data, explicit written consent of Data Subjects must be obtained unless an alternative legitimate basis for processing exists. The University understands "consent" to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

8.2 Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication.

8.3 In most instances consent to process Personal Data and Sensitive Personal Data is obtained routinely by the University (e.g. when a student enrolls or when a new member of staff signs a contract of employment, when an applicant submits an application). Such use is listed in the relevant data protection statement, or "privacy notice", which in the case of current students and staff are set out in the Student Handbook of Regulations and the Staff Handbook respectively.

8.4 Any University forms (whether paper-based or web-based) that gather Personal Data about an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed, or alternatively refers to the relevant privacy policy on the University's website where the individual can access further information. This requirement does not apply where Personal Data relating to a member of staff is being collected in connection with, and for the purpose of, that person's employment by the University. It is particularly important to obtain specific consent if an individual's Personal Data is to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.

8.5 If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

8.6 If any member of the University is in any doubt about these matters, they must consult the University Data Protection Officer.

9. Security of Data

9.1 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 11 on Disclosure of Data for more detail).

9.2 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:

9.2.1 in a lockable room with controlled access;

9.2.2 in a locked drawer or filing cabinet; or

9.2.3 if computerised, password protected.

9.3 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.

9.4 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.

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

9.6 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.

9.7 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.

9.8 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.

10. Rights of Access to Personal Data

10.1 All individuals have the right to access any Personal Data which are held by the University in electronic format and/or in manual records which form part of a relevant filing system, save where exemptions apply. This includes the right to inspect confidential personal references received by the University about that person.

10.2 Any individual who wishes to exercise this right should apply in writing to the University Data Protection Officer. The University reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee. In order to assist the University Data Protection Officer in complying with a Subject Access Request, it is helpful if the form provided through the University's Data Protection webpages is completed. For information on responding to subject access requests see the guidance available on the Information Governance website.

10.3 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.

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

11. Disclosure of Personal Data

11.1 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.

11.2 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.

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

11.3.1 the individual has given their consent (e.g. a student/member of staff has consented to the University corresponding with a named third party);

11.3.2 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);

11.3.3 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

11.3.4 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.).

11.4 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.

11.5 The DPA permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

11.5.1 to safeguard national security**;

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

11.5.3 assessment or collection of tax duty**;

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

11.5.5 to prevent serious harm to a third party; or

11.5.6 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, requests should be sent to the University Data Protection Officer.

11.6 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.

11.7 Unless consent has been obtained from the Data Subject, 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.

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

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

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

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.

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

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

12. Retention and Disposal of Data

12.1 The University discourages the retention of Personal Data for longer than it is required. Considerable amounts of data are collected on staff and students. However, once a member of staff or student has left the University, 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.

12.2 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.

12.3 The creation of systems and/or files which duplicate such data will be avoided; where it is inevitable every care will 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

12.4 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.

12.5 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

12.6 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).

12.7 Departments should regularly review the personal files of individual staff members in accordance with the University's Retention and Disposal Schedule.

12.8 Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for six months from the interview date. 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

12.9 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.

13. Publication of University Information

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

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

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

13.1.3 Awards and Honours (including Honorary Graduands, and Emeritus Professors and Prizewinners);

13.1.4 Staff Telephone and Email Directory;

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

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

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

13.2 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.

14. Direct Marketing

14.1 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.

14.2 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 this from happening once the University has received confirmation that a Data Subject has opted out.

15. Use of CCTV

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

15.2 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:

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

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

15.2.3 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

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

16. Academic Research

16.1 Personal Data collected only for the purposes of academic research (includes work of staff and students) must be processed in compliance with the DPA and in compliance with the University's Research Ethics Integrity policy and procedures.

16.2 Individual students or staff carrying out research should note that Personal Data processed ONLY for research purposes receive certain exemptions (detailed below) from the DPA **if**:

16.2.1 the Personal Data is not processed to support measures or decisions with respect to particular individuals; and

16.2.2 if any Data Subjects are not caused substantial harm or distress by the processing of the Personal Data.

16.3 If the above conditions are met, the following exemptions may be applied to Personal Data processed for research purposes only:

16.3.1 Personal Data can be processed for purposes other than that for which it was originally obtained, including statistical or historical purposes (exemption from Principle 2);

16.3.2 Personal Data can be held indefinitely (exemption from Principle 5); and

16.3.3 Personal Data is exempt from Data Subject access rights where the Personal Data is processed for research purposes and the results are anonymised (exemption from part of Principle 6 relating to access to personal data).

16.4 Other than these three exceptions, the DPA applies in full in respect of academic research. The obligations to obtain consent before using Personal Data, to collect only necessary and accurate Personal Data, to hold Personal Data securely and confidentially and not not disclose Personal Data except in accordance with the DPA (including in relation to publication) must all still be complied with.

Notes to Researchers

16.5 Whilst the DPA states that research may legitimately involve processing of Personal Data beyond the originally stated purposes (e.g. longitudinal studies), the University hopes that, wherever possible, researchers will contact participants if it is intended to use Personal Data for purposes other than that for which it was originally collected.

16.6 Although the DPA allows Personal Data processed only for research purposes to be kept indefinitely, researchers are asked to refer to their School's Research & Ethics panels for further guidance.

16.7 For those departments which gather Sensitive Personal Data, extra care should be taken to ensure that explicit consent is gained and that such Personal Data is held securely and confidentially so as to avoid unlawful disclosure.

Publication

16.8 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.

17. Further Information

Useful web addresses:

- University Information Governance pages
- Information Commissioner's Office
- JISC website
- JISC Legal – Data Protection and Research Data FAQs
- HESA data protection information

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

University of HUDDERSFIELD

Additional Guidance

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.

The guidance notes include the following:

- Data Protection - Key Points
- Handling Subject Access Requests
- Handling Third Party Requests for Personal Data
- References
- Use of Images
- Records Management