Z DATA PROTECTION AND PERSONAL FILE ACCESS POLICY

1. Introduction

The purpose of this policy is to enable the Hull University Union Limited (HUU) to:

- *Demonstrate its commitment to privacy, confidentiality and the proper handling of personal data*
- *Comply with Data Protection law*
- *Protect the organisation from the consequences of any breach of its statutory and common law responsibilities*
- *To encourage and support a culture of respect of privacy and data protection*

Managers are responsible for ensuring the Policy is properly understood and implemented by their staff, and for monitoring compliance. In addition, they must ensure that all procedures attached to this policy are implemented and followed.

Definition

Personal data is information that identifies a living individual, whether they are a student, a staff member, volunteer or other person connected to HUU (for example a job applicant or contractor). Data can include information stored in computer files, paper records, images, sound recordings and files, as well as correspondence like emails, letters, and notes. If there is any doubt about whether information is covered by this policy, staff must consult the Chief Executive.

2. Responsibilities

The Data Protection Act (DPA) applies to all staff, students, contractors and volunteers working for HUU. HUU is a Data Controller, as defined in Section 1 of the DPA, and is obliged to ensure that the DPA's requirements are implemented, monitored and evaluated.

Trustee Board

The Trustees of HUU have overall responsibility for ensuring that the organisation complies with its legal obligations.

Data Protection Lead

The officer in day-to-day control of Data Protection is the Chief Executive. His/her responsibilities are:

- *Briefing the Senior Management Group on their Data Protection responsibilities*
- *Recommending to the Board risk assessments to information across HUU*
- *Investigating incidents of breaches or alleged breaches of information security*
- *Dealing with all correspondence between HUU and the Information Commissioner's Office*
- *Reviewing and updating Data Protection and related policies*
- *Advising all staff on Data Protection issues*
- *Ensuring that Data Protection induction and training takes place*
- *Handling subject access requests*
- *Approving unusual or controversial disclosures of personal data to other organisations*
- *Advising on Records Management*
- *Overseeing implementation of the Records Management Policy*
- *Planning, undertaking or commissioning data protection audits*

Marketing and Communication Manager (M&CM)

The M&CM is responsible for electronic information security related to the student data base provided by the University and for ensuring the Data Sharing Agreements with the University and Lincoln Students' Union are complied with.

Managers

Managers are responsible for ensuring that this Data Protection policy and procedures are understood and implemented by their staff.

Data Owners

Data Owners are responsible for ensuring that information they are responsible for is protected appropriately, and where the information is shared that the proper confidentiality, integrity and availability safeguards have been applied.

Senior Management Team

Directors or equivalent are responsible for ensuring that this policy is communicated and implemented across their area of responsibility. They are responsible for the quality, security and management of personal data in use in their area.

All staff

All staff must read and comply with this policy. It forms part of the employee handbook. Significant breaches of this policy will be dealt with under HUU's disciplinary policy. Staff will at all times obtain, store and use personal data in compliance with the DPA principles, and in a confidential manner. Volunteers who knowingly or recklessly breach the policy will be suspended immediately from their role and be subject to HUU Student Disciplinary Procedure. Penalties for breaching the policy must be included in contracts with third parties.

Students

Students at the University may, during their day to day voluntary work gather or process personal information about other identifiable, living individuals (e.g. through the use of membership lists, trip registrations). Students have responsibilities under the Data Protection Act 1998 for any personal data relating to other people which they may access. They must ensure that their use of the data conforms with the Act's requirements and HUU's policy. Students are expected to treat personal data in a responsible and professional manner and not knowingly or recklessly disclose it. HUU will take a serious view of any breach of the Data Protection Act including consideration of disciplinary action.

3. *Data Protection*

H.U.U. is registered as a Data Controller with the Information Commissioner's Office (IFO) in accordance with the Data Protection Act. A copy of the registration document is held by the Chief Executive and the standard purposes for which data is held are:

- *(a) Personnel and Employee Administration*
- *(b) Purchase/Supplier Administration*
- *(c) Membership Administration of:-*
  - *(i) Clubs and Societies*
  - *(ii) Student Representation on University Committees, panels, boards and other representative bodies*
  - *(iii) Elections*
  - *(iv) Advice Centre clients*
- *(d) Verification of Students' identity*

(e) *Generation of Demographic reports*

3 The Data Protection Principles

The DPA contains 8 principles that regulate the use of all personal data, regardless of the reason for which it is obtained, used and shared.

Principle 1 – fair and lawful use of data

All students, staff and others whose data is processed by HUU must be properly informed of how their data is used, unless an exemption is identified. Application forms and other methods of gathering personal data must set out how data is used, including how and when it is shared.

Information about identifiable individuals must only be disclosed externally when necessary. Any requests for disclosure without consent must be handled in accordance with the Data Protection principles – any unusual request will automatically be referred to the Chief Executive.

Principle 2 – Use of data only for specified purposes

Staff must consult the Chief Executive before any personal data is to be reused for any purpose that is substantially different to that which it was obtained for.

Principles 3 & 4 - Personal data shall be adequate, relevant and not excessive, as well as kept accurate and, where necessary, up to date

All personal data processed by HUU must be fit for purpose. Managers must ensure that personal data held in any form is accurate and up to date. Data subjects will be consulted about whether the information held about them is still current. Application forms and other data gathering tools and processes will be reviewed regularly to ensure that they gather the right data to make appropriate and fair decisions, and do not obtain irrelevant data.

Principle 5 - Personal data shall be kept for no longer than is necessary

All information must be retained and disposed of in accordance with HUU's Retention and Disposal policy. For any information not covered by the policy, staff will consult the Chief Executive.

Principle 6 - Personal data shall be processed in accordance with the rights of data subjects

Subject Access

Individuals have a right to request their personal data held by HUU in whatever form. All such requests must be sent to the Chief Executive and will be dealt with according to the Subject Access Procedure. Information must not be withheld without the authorisation of the Chief Executive.

Inaccurate data

Any person who complains that their data is inaccurate will be asked to provide evidence. If the data recorded on the system is inaccurate and can be changed without materially affecting the record, the record must be amended wherever the mistake appears. Where an inaccuracy played a part in a decision, or has generally been repeated through a case history or chronology, staff will amend – but not remove – the inaccuracy wherever it occurs.

Section 10 notices

Where a person contacts HUU to request that any use of their data ceases because it causes them damage or distress, the request must immediately be passed to the Chief Executive or Union solicitor for consideration.

Principle 7 - Appropriate technical and organisational security measures must be taken

In general, security measures must include (but are not limited to) the following:

- *all personal data stored electronically will be protected from viruses and external access, and will be backed up in a safe environment*
- *all personal data must be removed from redundant hardware and media storage before the equipment is disposed of*
- *personal information must not be stored on portable or removable equipment or media unless encrypted (e.g. memory sticks, laptops, discs etc.)*
- *personal data must not be stored on computer hard drives unless network storage is not available*
- *access to all records (whether held on computer or paper) must be restricted only to those who need it. Access to databases and folders will be designated on a role basis, not across a whole team or area.*
- *access controls like passwords, smart cards and other similar tokens must not be shared between staff*
- *passwords and other security identifiers must not be written down*
- *when sharing personal data internally or externally, appropriate security procedures must be followed. If data sharing is routine and an HUU procedure does not already exist, standard security procedures will be created by the appropriate Data Owner.*
- *offices where paper records or equipment are stored must be secure, and adequate measures must be in place to prevent the loss or theft of records – measures include controlling access to premises, checking the identity of individuals visiting premises, and locking away paper records when not in use. Managers are responsible for assessing the security risks in premises where their staff work, and taking remedial action*
- *paper documents containing personal data must be disposed of through shredding or arranging confidential waste disposal when no longer required*
- *all actual and potential incidents involving personal data must be reported to the Chief Executive.*

Data Processors

When HUU uses a contractor to process personal data on its behalf, it must sign a data processing agreement that requires them to take adequate steps to comply with Principle 7. HUU retains legal responsibility for the actions of processors, and so staff managing contracts or procuring external services must ensure that security procedures are specified in the contract or in a separate agreement, and subsequently checked to ensure that they are being carried out.

Contracts must set out whether contractors processing personal data can use subcontractors; if subcontractors are allowed, they must be put under identical security obligations to the original contractor

Principle 8 – Transfers of personal data outside the European Economic Area must be specifically requested

Any staff member who seeks to send person identifiable information in any format to countries outside the EEA, must discuss this with the Chief Executive or Union Solicitor.

4 Audit and assurance

Statement of Internal Control

Heads of Department must confirm in writing that the policy has been properly implemented in their department annually and forward to the Chief Executive.

Privacy Impact Assessment (PIA)

HUU will carry out an assessment with all new projects, services and redesigned projects and services to consider whether a privacy impact assessment is required. The PIA process outlined in the Information Commissioner's guidance will be followed where the change involves significant adverse implications for privacy.

The manager of any new project or service with implications for people's privacy is responsible for carrying out a PIA with the assistance of relevant Data Owners.

Data Protection Audit

HUU will conduct regular compliance audits of major services and processes to ensure that the Data Protection Act is complied with.

5. Policy review

The Chief Executive will be responsible for ensuring that this policy and its associated procedures will be reviewed every three years and approved by the Board.

6. Rights of Employees

Employees have rights in respect of personal data held about them by HUU as follows:

(a) The right of subject access
(b) The right to prevent processing likely to cause damage or distress
(c) The right to prevent processing for the purposes of direct marketing
(d) Rights in relation to automated decision-taking
(e) The right to take action for compensation if the individual suffers damage by any contravention of the Act by use
(f) The right to take action to rectify, block, erase or destroy inaccurate data
(g) The right to make a request to the Data Protection Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

The Director of Membership Services & HR and individual Heads of Department are responsible for holding data under the appropriate security arrangements (see Principle 7 above). The conditions under which data may be released to individual employees are detailed in the Personal File Access Policy below. In all cases, data held must conform to the Data Protection Principles as detailed in the Act.

7. Personal File Access Policy

H.U.U. will maintain and keep up-dated, a file or files for each employee into which will be placed all the paperwork and records generated during each employees career; computerised files will likewise be maintained.

Such files contain a substantial amount of personal and private information and must therefore be kept carefully and treated confidentially.

Personal files are kept and maintained in accordance with the Data Protection Act and in line with the Standard Purposes as declared in the Union's Data Protection Registration. The principle purpose of holding personal data is for Personnel and Employee Administration, examples of which include:

(a) Recruitment, promotion, training, deployment and career development
(b) Contacting next of kin and arranging medical attention
(c) Compliance with Statutory requests from the Inland Revenue, DSS, Benefits Agency, etc
(d) Disciplinary purposes
(e) Provision of references

The Director of Membership Services & HR and individual Heads of Department are responsible for the safe and protected keeping of all personal files and data therein.

Personal files will be made available only to:

(a) The Director of Membership Services & HR
(b) The individual, on request (as detailed below)
(c) The individual's Head of Department
(d) The Chief Executive
(e) Such other Heads of Department as may require information for specific purposes
(f) The Payroll Administrator
(g) Medical Advisers retained by the Union
(h) The Secretary to the Chief Executive for updating purposes only
(i) The President

Should an individual wish to inspect his/her own file or files a written request to this effect should be made to the Director of Membership Services & HR. A request will normally be granted within 5 working days, though in certain circumstances such inspection may need to be delayed. Any delay will be kept to a minimum. The Manager of Membership Services & HR will obtain from relevant Heads of Department details of data held and will make this data available to the individual, subject to the exemptions detailed below.

The inspection must take place within the Manager of Membership Services & HR's office and no part of any file may be removed or copied. All papers should be kept in the same order in which they appear in the file. Inspection will be supervised by the Manager of Membership Services & HR.

Should an employee disagree with an item or items of data included in their file, they should notify the Manager of Membership Services & HR in writing. The Manager of Membership Services & HR will then be responsible for investigating the matter and making a decision regarding the data. The decision will be communicated in writing within 7 working days. Should the request to alter or remove the data be refused, the employee will be notified with reasons for the decision. If the employee does not agree with the decision the matter should then be pursued under the Union's Grievance Procedure. If the employee remains dissatisfied following the full application of the Grievance Procedure, he/she retains the right to make a request to the Data Protection Commissioner for an assessment to be made as to whether any provision of the Data Protection Act 1998 has been contravened.

Certain classes of data are exempt from the right of subject access. These include:

(a) Employment references given by the Union in respect of the employee.
(b) Educational references.

(c) *Information that cannot be disclosed without also disclosing information relating to another person.*
(d) *Data contained within unstructured files which is not readily accessible.*
(e) *Data related to management forecasting or management planning.*
(b) *Data relating to any negotiations between the Union and the data subject where disclosure is likely to prejudice those negotiations.*

Appendix 1
Practical Implementation of the Data Protection Policy

Data Protection Procedures

The following policies and procedures are to be read in conjunction with the Data Protection Policy:

(a) Using paper records out of the office
(b) Providing personal information safely by email
(c) Faxing personal information safely
(d) Providing personal information safely over the phone
(e) Sending personal information in the post
(f) Contractor Checklist – third party processing
(g) Managing requests for access to personal records
(h) Managing requests for personal information from third parties
(i) CCTV
(j) Research involving data gathered from human participants or from records
(k) Information Security Breach Management Procedure
(l) Retention and disposal

(a) Using paper records out of the office

If staff need to use paper records containing personal or other confidential data out of the office, the records must be kept safe at all times. An encrypted laptop or other form of remote, secure access to information may be a safer alternative and will always be considered.

Basic principles

- *Managers will approve in principle the circumstances in which paper records are removed from the office and by whom.*

- *Personal/confidential records will be removed only where necessary, and only for the minimum time required. They will be returned as soon as possible.*

- *Staff carrying paper documents containing personal/confidential information are responsible for their safety – even if they are carrying documents for someone else.*

- *Personal files or folders will only be removed if they are in a safe and transportable state. There will be no loose papers. A file that is damaged or too large will be re-filed before being taken out.*

- *Personal files or documents will be carried in a secure bag at all times when out of the office. Wherever possible personal/confidential documents will be carried in a lockable,*

waterproof bag. An open shopping or carrier bag is never an appropriate way to carry personal data, or confidential or sensitive documents

- *Where larger quantities of personal/confidential records are routinely removed from the office, they will be kept secure at all times, for example carried in a lockable wheeled case.*

- *Staff will refrain from reading files or records containing personal data on public transport, in restaurants or cafes, or anywhere else where they can be overlooked.*

- *Never leave personal files, documents or folders unattended, or on show in a car or other vehicle*

- *Before leaving any building, car or public transport, and before you drive away from any location where you have been using paper records, make a conscious check that you have retrieved everything.*

- *Never leave paper records in your car overnight. If you need to return home with documents containing personal or sensitive data, take them into your home and keep them safe. Ensure that family members do not read or access them.*

- *If you leave records at home for any reason when you are not there, they will be locked away*

(b) Procedure for providing personal information safely by email

- *When sending sensitive information (e.g. information about criminal activity, health or other potentially damaging information), use an encrypted email system.*

- *If password-protecting a document, do not send the password by email – contact the recipients separately to provide the password, and change it every time. Be aware that passwords can easily be broken if they are a dictionary word or simple combination of letters or numbers*

- *Check that you have the right email address*

- *If sending personal or sensitive data, ensure you check the recipient's address - eg type the whole address in yourself, or choose it from an address book. If you have previously emailed a person with a similar name to your current recipient, be aware that Outlook and similar packages might fill in the wrong name*

- *If you are copying a number of people into an email, always use the BCC ('blind copy') function unless you are certain that each recipient already knows the other's address. If you are sending emails to multiple people's home addresses, use BCC regardless. It can be a breach of privacy to reveal a person's home email address*

- *If using a distribution list, check before sending the email that you have selected the correct email addresses.*

- *Check that you have added the right attachment before sending an email*

- *Ensure that the language and tone of an email is appropriate – an email can be treated by a court like a signed letter on headed paper. You will assume that this might happen to your email. Any email containing personal data may be requested by the person under the Data Protection Act 1998.*

(c) Procedure for faxing personal information safely

For both confidentiality and legal reasons, it is vital that care is taken when faxing personal information about individuals. Individuals are entitled to expect that their privacy and confidentiality is respected, and that their data is always treated with care and appropriate security.

Staff, volunteers and contractors

- *Ask yourself this: will I send this as a fax, or is there a safer alternative?*

- *Always use a cover sheet marked 'Private and Confidential' and which contains:*
  - *A named recipient, or at least a team name who the fax is for*
  - *Your name, job title, team, location, your telephone number and fax number*
  - *The number of pages you are sending, including the cover sheet*
  - *an explanation of what to do if the fax has been received by the wrong person (e.g. contact you immediately, and do not read or share the contents with anyone else)*

- *Before you send the fax, telephone the intended recipient to let them know you are sending a confidential fax*

- *Always keep transaction reports as evidence of where the fax was sent in case it was sent to the wrong person, so you have a chance of contacting the recipient*

- *Ask the recipient to ring you back to confirm receipt, or ring them yourself after you have sent the fax*

- *Make sure they confirm that all pages have been received*

- *If using a pre-programmed fax number, ensure that you choose the right one, and regularly check that the pre-programmed numbers are still correct*

- *If you are entering the number manually, double-check it to make sure you are using the right number*

Managers

- *You will be aware what data is contained in the faxes your staff are sending, who they are sending them to, and why fax is being used as an alternative to other methods. You will review whether fax remains the right way to share information – secure email may be a more secure alternative.*

- *Your fax machine will be in a restricted location, not in a public area of your building where faxes can be picked up by anyone who is not part of your team or not authorised to see the information that is being received – if staff pick up your faxes from a central location, they must be trained not to read the faxes, and to bring them straight to your team. You will consider whether this arrangement is secure.*

- *You will ensure that a member of your team regularly checks any pre-programmed numbers to ensure that they remain correct and up-to-date*

(d) Procedure for providing personal information safely over the phone

When someone calls you asking for personal information:

- *Identify the person clearly, check who they are, who they work for and what they want*

- *If they demand information, check their entitlement to demand it – ask what law or right allows them to demand the information. More information on this topic is included in Section H.*

- *Unless you are certain that the person is who they say they are, get their switchboard number (not their direct number) and ring them back. Check the switchboard number from their website, not from them*

- *If in doubt, ask them to put their request in writing*

When you call someone to provide personal information:

- *Be certain that the phone is the best way to provide personal information – would a fax or email be better (both allow a specific record of the information to be provided)*

- *Ensure you speak to the person who needs the information – do not leave personal or sensitive data in a message*

When someone calls to provide you with personal information:

- *Ensure you record information accurately – check the information with the person providing it. Do you have the spelling, numbers and details right?*

(e) Procedure for sending personal information in the post

When sending out paper documents containing personal data, you must ensure that documents are secure and properly addressed. The person sending the document is responsible for ensuring that they are sent to the right people, safely packaged, and that they can safely be returned to you if not delivered.

For staff, volunteers and contractors

YOU MUST:

- *Ensure that the destination you are sending documents to is still in the same place – especially if the recipient is outside the University.*

- *Check the address to ensure that it is correct, and send documents to a named person if at all possible, and not to a department or team.*

- *Never address a letter or package containing an individual's personal data to an organisation without at least identifying the team.*

- *Always put either a covering letter or a compliment slip with your contact details in the envelope with the information – DO NOT put personal records or data into an envelope by themselves.*

- *Write your return address on the back of the envelope – this will allow a wrongly delivered envelope to be returned without having to be opened*

- *Seal the envelope securely and mark it 'Private and Confidential'*

- *Send any personal or other sensitive information by recorded delivery, and keep the tracking information so you can find out when it was delivered*

For managers

If your team are routinely sending out large volumes of personal data, you will consider how the process can be made more secure. The use of taxis to ferry information is unsatisfactory, and you will consider, for example, whether a contract with secure couriers would be more appropriate.

(f) Contractor checklist – third party data processors

A data processor may be a courier who you regularly use to transfer your records, an IT specialist coming in to work on your systems, a consultant or a contractor to whom you outsource work, projects or services. If they handle, analyse, cleanse, send out, shred or collect data for your purposes, you will always ask these questions BEFORE you complete a contract. No matter how good a job your contractor does, if you do not get security protections in writing, you do not have them. They are not liable for security breaches – you are.

1 *Have you got a written agreement or contract with your processor, which sets out what the job is, and how any personal data will be used?*

2 *Does it include guarantees that the contractor has adequate security in place to look after your data?*

3 *In general, is the security set out in the contract at least as strong as the security you have in place when using the data you intend to supply to them?*

4 *Have you specifically set out what security arrangements they will put in place? This will depend on the arrangement, but some examples include:*
   - *Have you insisted that any laptops, pen drives or other portable media are encrypted?*
   - *Have you required the contractor to put in place appropriate security when moving paper records around?*
   - *Have you insisted on secure storage when personal data is held at their premises – does paperwork need to be locked away, is information stored on systems which have anti-virus protection, back-ups and firewalls*

5 *Have you set out what will happen to data when the project is completed – i.e. destroy data with confirmation or return all copies to you?*

6 *Have you set out restrictions on what the contractor can do with the data, with whom they can share it, and which of their staff is entitled to access and use the data?*

7 *Have you confirmed that the contractor cannot use the data for their own purposes, and cannot disclose it to a third party without your express permission?*

8 *Have you put in place a mechanism to ensure that the contractor is doing what they have agreed to do?*

(g) Managing requests for access to personal records

See Section 6 above for staff. For students, any request will be passed to the Chief Executive who will decide what information may be safely provided.
Under normal circumstances students will be in a position to know what information is held about them and have an opportunity to correct it if necessary.

Under the legislation, a data subject (students) may request details of all information held about them. A formal request from a data subject for a copy of such information will include the following:

i) the request in writing, indicating what information is being sought

ii) the appropriate fee (if any)

iii) enough information for HUU to be sure of the identity of the data subject and to locate the information. For example, in the case of a former student, it would be reasonable for them to provide the dates of their period(s) of study, details of their course(s) and, if possible, their student registration number.

The CE will instigate a search and respond to the data subject within 40 days of receipt of the request, payment and information.

If holders of information requested by a data subject wish to withhold it under any exemption included in the Data Protection Act 1998, they will seek a ruling from the CE or the Union's Solicitor.

Exemptions from the right of subject access:

References given by the Union are exempt from the right of subject access.

(i) CCTV

HUU has a comprehensive CCTV surveillance system in University House. Cameras have been installed and system is owned by the Union. A Code of Practice has been prepared for guidance of managers and the operators of the CCTV system. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the HUU, consistent with the obligations on HUU imposed by the Data Protection Act 1998.

(j) Research involving data gathered from human participants or from records

*8.1. **The status of personal data processed for research purposes only**. The fifth data protection principle states that 'personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'. This poses problems for research because data gathered in the course of a research project are fundamental to the validation of the project, both as it is completed and in the future, as questions raised by the results of the research are revisited over time. The Data Protection Act allows for this situation by granting an exemption from the fifth data protection principle. The exemption allows personal research data to be retained indefinitely, but only as long as a) the data is not processed to support measures or decisions taken at some future time with respect to particular individuals, and b) the data is not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.*

*8.2. **Archiving personal research data**. The Act also allows secure archiving of data gathered for a particular research project in recognition of the fact that the data may have further research uses not apparent at the time of collection ('the further processing of personal data only for research purposes in compliance with the relevant conditions ... is not to be regarded as incompatible with the purpose for which they were obtained'). There is also an exemption from the need to inform data subjects about the further processing of their data for research purposes provided that the data is processed in compliance with the relevant conditions and the results of the research, or any statistics arising from the research, are not made available in a form which identifies any data subject. Advice on disposal or archiving of research data, and access to data by third parties, once the purpose for which they were collected no longer applies, may be obtained from the Chief Executive.*

*8.3. **Limiting the nature of personal data collected**. Only data necessary for the conduct of the study will be collected. In particular, data of a sensitive nature will not be requested unless genuinely necessary. This includes data on racial or ethnic origin, political or religious beliefs, membership of a trade union, physical or mental health, sexual life, criminal offences, proceedings or conviction. If such data is not absolutely necessary for the research study, do not collect them.*

*8.4. **Use of anonymous data**. In many circumstances it is not necessary to record the identity of the individual who provides the data for research. Data is exempt from subject access where results or statistics do not identify the individuals from whom the data is obtained. Therefore careful consideration must be given at the time a research project is planned as to whether the identities of the participants are required or whether it would, for example, be sufficient to note certain facts about the participant that would not allow them to be identified as individuals. In many situations, the research project does not require the identity of the participants to be noted, in which case the source of the data can remain anonymous.*

*8.5. **Disclosing research data**. Researchers will be aware that if research data is not collected anonymously so that it is possible to link the data to identifiable individuals, then the Act grants those individuals a right of access to the data. This would be done by making a data subject request. Thus, test results, medical information, questionnaire responses, and other data provided by participants are disclosable where the identity of the participant is retained. This includes a situation in which a separate list or key kept within the institution makes it possible to link research data to an identifiable individual.*

*8.6. **Transferring research data**. Where possible the transfer of data relating to identifiable individuals to other researchers outside the institution will be avoided. In particular it is advised that non-anonymised data will not be transferred to countries outside of the European Economic Area.*

(k) Information Security Breach Management Procedure

The Data Protection Act 1998 (the Act) governs the HUU's obligations with regard to personal data and these include a requirement to keep personal data secure. A breach of data security occurs where unauthorised or unintentional access to personal data is gained, whether this data is held in electronic or manual format.

How can a breach occur?

A breach can happen as a result of:

- *Loss or theft of data held manually or stored on equipment or a physical device e.g. a USB stick or CD*
- *Inappropriate access controls allowing unauthorised use*
- *Equipment failure*
- *Human error*
- *Unforeseen circumstances such as fire or flood*
- *A hacking attack*
- *Blagging offences where information is obtained by deceiving the organisation holding it*

Consequences of a breach

A breach could damage HUU's reputation and its relationship with its stakeholders or expose HUU, its staff or students to the risk of fraud or identity theft. In addition, considerable distress could be caused to the individuals concerned, as a result of which HUU could be sued.

Breaches of the Act have become an increasingly high profile issue in recent years and in addition to enforcement action, the UK Information Commissioner (ICO) who oversees the Act, currently has powers to impose civil monetary penalties up to a maximum of £500K and this is likely to increase.

Procedure

1. Discovery of a breach

1.1 In the event of a breach occurring with personal data which is held in either electronic or manual format, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

1.2 Staff must notify their line manager as soon as possible of any breach. The line manager will notify their Head of Department. The Head of Department, Data Owner, or other senior member of staff in the area in which the breach has occurred, must ensure that the Chief Executive is notified as soon as possible.

1.4 The Chief Executive will decide, based on the particular circumstances of the breach, whether it is serious enough to inform the Trustee Board and will liaise as appropriate with any other key staff.

1.5 The Head of Department, Data Owner or other senior member of staff in the area must establish the following:

- *the exact nature of the breach*

- *the number of individuals who have been affected by the breach*

- *what steps need to be taken to contain the breach*

1.6 The Head of Department, Data Owner, other senior member of staff, Chief Executive and where applicable the University Registrar and Secretary, will decide in consultation with any other relevant staff on the immediate actions to be taken to contain the breach.

2. Managing the consequences

2.1 The Chief Executive will consult with the Head of Department or Data Owner, and others if necessary and will then seek the Trustees' decision on whether to inform:

- *The UK Information Commissioner*

- *The individuals who may have been affected.*

2.2 Prior to individuals being informed, the MM&C will be consulted. HUU will explain the situation and the steps being taken to protect their personal details.

2.3 A report of the breach will be made to the next meeting of the Trustee Board, providing an overview of the breach, lessons learned, related actions and timescales.

(l) Retention and disposal policy

It is a requirement of the Data Protection Act 1998 that all information relating to identifiable living individuals will be kept for no longer than necessary and then disposed of in an appropriately secure manner.

Records that are hold whether they are paper based or stored on an electronic or digital format will be regularly reviewed to ensure they are still valid and need to be kept.