LIVERPOOL HOPE UNIVERSITY

Data Protection Policy

v2 - revised:	November 2013
Approved by:	University Council
Date of Approval:	26th November 2013

Introduction

The University needs to keep certain personal data, for example about its staff and students, to fulfil its purpose and to meet its legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the University must comply with the eight Data Protection Principles which are set out in the Data Protection Act 1998.

Principles

Personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights under the Act.
- Be kept secure from unauthorised access, unlawful processing, accidental loss or destruction through appropriate technical and organisational measures.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for the rights and freedoms of data subjects in relation to the processing of their personal data.

The University and all its staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the University has developed this Data Protection Policy.

Status of the Policy

This policy has been approved by the University Council of Liverpool Hope University and any breach will be taken seriously and may result in instigation of disciplinary action.

Any member of staff or student who considers that the Policy has not been followed in respect of personal data about themselves should raise the matter with the University Data Protection Officer in the first instance. Contact details for the Data Protection Officer are provided at the end of this document. The Data Protection Officer will be responsible for conducting an investigation into any reported breaches of the policy, in line with ICO guidance on information security breach management

Notification of Data Held and Processed – Privacy Notice

All staff, students and other users are entitled to:

- Ask what information the University holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what the University is doing to comply with its obligations under the Data Protection Act 1998.

Responsibilities of Staff and Students

All staff and students are responsible for:

- Checking that any personal data that they provide to the University is accurate and up to date.
- Informing the University of any changes to information which they have provided, e.g. changes of address.
- Checking any information that the University may send out from time to time, giving details of information that is being kept and processed.

If, as part of their responsibilities, staff collect information about other people (e.g. about students' course work or personal circumstances, or about members of staff in their department or research group), they must comply with the Policy and with the Data Protection Guidance Notes.

Students who use the University computer facilities may, from time to time, process personal data. If they do so they must notify the University Data Protection Officer.

Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Detailed advice on data security is contained in the Guidance Notes below. The University has also developed an Information Security Policy which provides further guidance:
http://www.hope.ac.uk/aboutus/governance/policiesandstrategies/

Rights to Access Information – Subject Access Requests

Staff and students and other users of the University have the right to access any personal data that is being kept about them on computer and paper or manual records which are kept in an organised filing system. Any person who wishes to exercise this right should submit a Subject Access Request (SAR) in writing, using a standard form which is available from the University Data Protection Officer. The University will make a charge on each occasion that access is requested.

The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a completed form and payment unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

Publication of University Information

Information that is already in the public domain is exempt from the Act. Any individual who has good reason for wishing details in such publications to remain confidential should contact the University Data Protection Officer.

Under the Act staff and students have rights of access to the data held by the Higher Education Statistics Agency (HESA) . You will have to pay a small fee for this. For further information about the HESA record please see www.hesa.ac.uk/dataprot or email data.protection@hesa.ac.uk

Subject Consent

The need to process data for normal purposes is communicated to all staff during induction, and to all students during the registration process. In some cases, if the data is classed as sensitive, for example information about health, race or gender, then express consent to process the data must be obtained. Processing may be necessary to operate University policies, such as health and safety and equal opportunities.

Retention of Data

The University will keep some forms of information for longer than others, in accordance with retention schedules outlined in the University's Records Management Policy:
http://www.hope.ac.uk/aboutus/governance/policiesandstrategies/

The University's Designated Data Protection Officer

The University is the data controller under the Act and is therefore ultimately responsible for implementation. However, day to day matters will be dealt with by the University Data Protection Officer. Any questions or concerns about the interpretation or operation of this Policy should be taken up in the first instance with the University Data Protection Officer:

Mr Graham Donelan
University Secretary
Liverpool Hope University
Hope Park
Liverpool
L16 9JD
Tel: 0151 291 3756
Email: donelag@hope.ac.uk

DATA PROTECTION POLICY

GUIDANCE NOTES

The purpose of these guidance notes is to underpin Liverpool Hope University's Data Protection Policy and to provide advice on best practice in relation to Data Protection.

Data Protection Act 1998

1. The Data Protection Act 1998 builds upon and expands the controls on personal data established under the 1984 Data Protection Act. The 1984 Act introduced basic principles of data protection, which set standards that all registered users were required to observe. It was designed to protect individuals from any disadvantage which might result from their personal details being held on computer, for example if the information became out of date, was lost, or was made available to people or used for purposes other than those it was collected for. The Act also set up the framework for compulsory registration of data users, and established the Data Protection Registrar to organise this process and to ensure compliance.

2. Under the 1998 Act, the data protection principles were extended and 'personal data' includes information held in certain manual filing systems. Individuals are given enhanced rights to receive details of data held about them and why it is being held, and to prevent its use. The processing of data will only be fair if certain conditions have been met, and some information is classed as 'sensitive data' and there are particular restrictions on the use of it. There are also restrictions on the transfer of data to countries outside the European Economic Area. The 1998 Act replaced the office of the Data Protection Registrar with that of the Information Commissioner, and the registration of data users was replaced by notification.

3. The provisions of the 1998 Act became fully effective on 23 October 2007. Records in new filing systems created after October 1998 are covered by the 1998 Act.

Notification

4. Under the 1998 Act, the University is required to register with the Information Commissioner's Officer as a data controller. Registration by a data controller includes details of the classes of person whose data may be held, the purposes for which it is held, the sources from

which it may be obtained, and the classes of persons to whom it may be disclosed. Details of the University's current registration can be accessed on the Public register of data controllers available from the Information Commissioner's Office website at http://www.ico.org.uk.

The University's registration is reviewed and updated annually. *If a new project involving personal data is being set up, or data already held are to be made available to different categories of people or used for a different purpose than the original, the person responsible must inform the University Data Protection Officer. (See the end of this document for details of how to contact this person).*

Any formal requests under the Act from data subjects regarding information held on them (Subject Access Requests) must be referred to the University Secretary, no matter which individual, office, School, Faculty or service unit is processing the information.

Staff Guidelines for Data Protection

5. All staff will process data about students on a regular basis, when marking registers, marking coursework and examinations, writing reports or references, or as part of a pastoral or academic supervisory role. The University will ensure, through registration procedures, that all students are informed that the University undertakes this sort of processing, are notified of the categories of processing, as required by the 1998 Act. The information that staff will deal with on a day to day basis will be 'standard' and will cover categories such as:

- **General personal details e.g. name and address**
- **Details about class attendance, course work marks and grades and associated comments**
- **Notes of personal supervision, including matters of behaviour and discipline**

6. Information about a student's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity or race is classified as 'sensitive' data and can only be collected and processed with the student's consent. This might be required, for example, for health reasons prior to taking students on a field trip, or for pastoral duties when a student has health problems.

7. Staff may also collect and process data about other staff in the University. Deans may, for example, process data about the staff in their Faculty, or research group leaders may process data about the members of their groups. The University will ensure that all staff are notified of the types of data held on them and the categories of processing. Most of the information collected will be standard data, but if, for any reason, sensitive data, as set out in paragraph 6, is required

to be collected and processed, then the express consent of the individuals concerned must be obtained.

8. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the University Data Protection Policy. In particular, staff must ensure that records are:

- **Accurate**
- **Up-to-date**
- **Kept and disposed of safely**

9. Staff must not disclose personal data unless for institutional purposes in line with University policy. The policy prevents disclosure to a third party (including a concerned parent) unless written consent has been obtained from the subject. The only exception to this will be if a member of staff is satisfied that the disclosure of the personal data is necessary:

- In the best interests of the student or staff member, or a third person, or the University AND
- He or she has either informed the Data Subject of this, or has been unable to do so and disclosure is urgent and necessary.

This should happen only in exceptional circumstances, e.g. medical emergency.

Data Security

10. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff should ensure that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party

11. All personal information in the form of manual records should be:

- Kept in a locked filing cabinet: or
- Kept in a locked drawer

If information is stored electronically, it should be:

- Password protected, with passwords being regularly changed, so that only authorised people can view or alter confidential data; or

- Kept only on a disk which is itself kept securely in a desk or cabinet to avoid physical loss or damage

12. To avoid unauthorised disclosure, care must be taken to site PCs and terminals so that they are not visible except to authorised people. Screens should not be left unattended when personal data is being processed. Similarly, care must be taken to ensure that manual records, e.g. staff or student files, or printout containing personal data, are not left where they can be accessed by unauthorised staff.

13. When manual records, or printout containing personal data, are no longer required, they should be shredded or bagged and disposed of securely.

14. Particular care must be taken of any data taken away from the University, for example manual records to be used at home, or computerised data to use on home machines or on portable devices, including smartphones and tablet PCs. Ensure that all work is kept confidential and, in the case of computerised information, that files are not exposed to risk from virus infection.

15. When personal devices are used for work purposes, a strong password should be used to secure the device and encryption should be enabled to store data on the device securely. Staff should ensure that access to the device is locked or data automatically deleted if an incorrect password is input too many times.

Use of Personal Data for Research Purposes

16. The 1998 Act provides for exemptions for personal data processed for academic, scientific, historical or statistical research. Provided that personal data has been obtained fairly and lawfully, then the subsequent use of that data for research purposes will not breach the second data protection principle. Data collected for the purposes of one piece of research can be used for other research, and may be kept indefinitely. However, there must be no direct consequences for the individuals in respect of whom the research is carried out and the personal data must not be processed in a way which is likely to cause damage or distress to any data subject.

17. In order to avoid subject access provisions, the results of research or statistics should not be made available in a form which identifies the individuals concerned. Wherever possible, researchers should follow a principle of 'pseudonymity' in handling personal data and, for example, avoid the storage of names and addresses directly on computer by relying on reference codes instead.

Provision of References

18. Care should be taken when writing confidential references. Under Data Protection legislation, a confidential reference given by the University to a third party, for the purposes of education, employment, training, appointment to a public office or any service being provided by the individual who is the subject of the reference, should remain confidential and is exempt from the subject access provisions, in that the subject cannot gain access from the person writing the reference. However, there are occasions when references will have to be disclosed, for example in a court of law.

19. Once employed at the University, members of staff will be able to submit a Subject Access Request to see the reference held on their Personnel File

Staff Checklist for Recording Data

20. Before processing any personal data, all staff should consider the following checklist:

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- Have you checked with the data subject that the data is accurate?
- Are you sure that the data will be secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or staff member to collect and retain the data?

Staff Checklist for Sharing Data

21. Before sharing any personal data, all staff should consider the following checklist to ensure that the sharing complies with the legislation and meets individuals' expectations

- Is the sharing justified?
- Do you have the authority to share the information?
- Is a data sharing agreement in place?
- What information do you need to share?
- Ensure that the method of sharing information is secure
- Consider whether it is appropriate to inform the individual that you have shared their information
- Record your data sharing decision and your reasoning