University of Liverpool

Data Protection Policy

Reference Number	
Title	Data Protection Policy
Version Number	1.0
Document Status	Active
Document Classification	Open
Effective Date	June 2018
Review Date	May 2019
Author	Vicki Heath
Approved by	Council
Implemented by	Data Protection Officer
Monitoring of compliance	Legal & Compliance
Comments	

Table of Contents

Data Protection Policy

Introduction

The University processes large volumes of personal data in relation to its staff and students, to fulfil its purpose and to meet its legal obligations to funding bodies and government. It also processes personal data of participants in research projects. 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 Data Protection Principles which are set out in the Data Protection Act, 1998 or 'the Act' and from 25 May 2018 the General Data Protection Regulation (GDPR).

This is one of a suite of policies that aims to ensure the University is compliant with GDPR and has a robust Information Governance framework.

The GDPR introduces strengthened rights for individuals, greater sanctions for breaches and an accountability requirement for data controllers to demonstrate compliance and robust governance. The data controller decides on the nature, scope, context and purpose of processing the data, whereas a data processor acts only on instruction from a data controller and processes data on behalf of the data controller. The University is a data controller and in some instances may be a data processor.

What are Personal Data?

Personal data means *information about a living individual, who is identifiable by the information, or who could be identified by the information combined with other data*, which the University has or may have in the future. Furthermore, any recorded *opinions about* or *intentions regarding a person* are also personal data; and this includes both student progress reports and staff review reports.

Special categories of personal data or sensitive personal data is information relating to mental and physical health, ethnicity or race, religious and political beliefs, trade union membership, sexual orientation or biometric or genetic data.

The main data the University processes is:

Staff Data

Student Data

Research Data

Principles

Personal data shall be:

- Processed lawfully in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary
- Accurate and where necessary, kept up to date and every reasonable step taken to erase or rectify inaccurate data
- Kept in a form which permits identification of data subjects for no longer than necessary

- Processed in a manner that ensures appropriate security

From May 2018 there is a new principle of accountability for data protection compliance which means that the University must be able to demonstrate how it is complying with the GDPR.

The University and all its staff and students 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. The legislation covers ALL personal data processed by the University, electronic or hard copy, irrespective of whether these are held by individual members of staff or students in their own separate files (including those held outside the University campus) or in departmental or faculty records systems.

The GDPR place restrictions on what the University can do with personal data; certain conditions, which include obtaining data subject consent, must be met before processing can take place. The term 'processing' covers almost anything that is done to data by reference to individuals and the practical implications of these restrictions are wide-ranging.

Status of the Policy

This Policy has been approved by the University Council and any breach will be taken seriously and may result in disciplinary proceedings.

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, Vicki Heath, in the first instance. It is a mandatory requirement to report any serious data breaches to the Information Commissioner's Office within 72 hours. These should be reported in the first instance to the Data Protection Officer who will liaise directly with the ICO.

Right to be Informed

All staff and students are entitled to know:

- The identity and contact details of the data controller
- Purpose of the processing and the legal basis
- Any recipients of the data
- Details of transfers to third country and safeguards
- Retention period
- The right to lodge a complaint
- The existence of automated decision making

Rights to Access Information

Any person who wishes to exercise this right should make the request in writing to the University's Data Protection Officer, using the standard Data Protection Enquiry/Subject Access Request Form via LegalServices@liverpool.ac.uk.

The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 calendar days of receipt of a completed form 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.

Right to Erasure / Be Forgotten

In certain specific circumstances individuals can request deletion of their data. However, the instances where this right will apply to data processed by the University will be very few, especially as the University has legal obligations to keep a central record of all staff and students.

Any person who wishes to exercise this right should make the request in writing to the University's Data Protection Officer, via LegalServices@liverpool.ac.uk.

Right to Data Portability

Individuals are also entitled to receive their data in a structured, commonly used and machine readable format so it can be transmitted automatically to another data controller. This applies only to information that has been originally provided by the individual themselves and is being processed by automated means for the purpose of a contract (so potentially student or staff data).

Any person who wishes to exercise this right should make the request in writing to the University's Data Protection Officer, via LegalServices@liverpool.ac.uk.

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 (students) or updating changes through the CORE HR portal (staff).
- 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' personal circumstances, or about members of staff in their department or research group), they must comply with this Policy.

Personal Research Data

Staff are responsible for applying this policy to any personal data they acquire during research studies undertaken by themselves or by students under their supervision. Any staff or student research project that collects personal data from participants in the study must have formal ethical approval before it begins. Participants must be informed on how the data being collected will be stored, preserved and used in the long term, and give their consent to this use of their data. Personal data collected during research studies should be held in a fully anonymised form that protects the confidentiality of its participants.

Data Security

It is the responsibility of the University to ensure that appropriate technical and practical measures are taken to safeguard personal data held from loss, damage or destruction. Failure to do so could result in financial and reputational damage to the University. 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 they adhere to the University's Information Security Policy. Generally staff should ensure that:

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

All staff are required to complete the Information Governance training module upon employment and at regular intervals afterwards.

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 computerised, it should be:

- Securely stored on the MWS drive and documents additionally password protected, so that only authorised people can view or alter confidential data; or
- Kept in a restricted access folder and only sent electronically if encrypted.

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 and should be locked when they are unattended. Similarly, care must be taken to ensure that manual records, e.g. staff or student files, or printouts containing personal data, are not left where they can be accessed by unauthorised staff.

When manual records, or printouts containing personal data, are no longer required, they should be cross-cut shredded and disposed of securely in the confidential waste bins.

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 portable computers or home machines. Ensure that all work is kept confidential and, in the case of computerised information, that files are not exposed to risk from virus infection.

Mobile Devices

- Mobile devices should be purchased through CSD who provide phones and through Academia for tablets.
- This has the important security benefit that devices bought through the University are encrypted as routine. Similarly any devices connected to the Managed Windows Service will be encrypted.
- Staff may use their own devices to access email and the MWS system
- Staff who purchase devices out with of this process should contact CSD to ensure that the devices have the appropriate security measures.

Publication of University Information

Information that is already in the public domain is exempt from the Act. This would include, for example, information on staff contained within externally circulated publications. Any individual who has good reason for wishing details in such publications to remain confidential should contact the University Data Protection Officer.

Legitimate Interests

The need to process data for normal purposes has been communicated to all staff, in employee contracts, and to students at induction and registration and in student contracts. In some cases, if the data is sensitive, for example information about health, race or gender, 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. For more information about this please see the University Privacy Notice.

CCTV and Monitoring of Communications

For reasons of personal safety and to protect University premises and the property of students and staff, and to ensure that the University's resources are not abused, closed circuit television cameras are in operation in certain campus locations. Recordings are kept for either 7 days for analogue or 28 days for I.P. system recordings. If an incident is reported, images are provided to the campus police officer.

Students or staff who consider that the positioning of a CCTV camera is inappropriate should contact the Data Protection Officer.

Lecture Capture

Most University lecturers use cameras to record lectures so that they may be accessed and viewed online. More detail can be found in the Policy on Lecture Capture. However, careful thought should be given to potential problems arising from the public videoing of lectures and speeches such as the Vice Chancellor's address. In such circumstances, consent should be obtained from individuals attending or an appropriate warning sign should be posted within the area covered by the camera.

The University may from time to time monitor staff and student communications without giving notice to ensure compliance with the IT Appropriate Use Policy; random monitoring of personal computer usage, however, will apply only to publicly-accessible computer clusters; and random monitoring of telephone calls will not take place.

In any case:

- any monitoring will be carried out only by a limited number of staff
- personal data obtained during monitoring will be destroyed
- staff involved in monitoring will maintain confidentiality in respect of personal data.

Social Media

When using social media on behalf of the University eg Twitter the Social Media Compliance Policy is followed.

Retention of Data

The University will keep some forms of information for longer than others. The University has a Records Retention Schedule, which can be obtained via the web at
http://www.liverpool.ac.uk/csd/records-management/retention-schedule/

It is good practice to regularly review and delete emails to ensure that personal data is not kept for longer than necessary. Any emails required to be kept should be saved into files on local drives on the MWS rather than stored in Outlook.

Third Party Providers

The University contracts with third parties certain functions that involve the processing of personal data, such as the payroll function. It is a requirement in these circumstances for a written contract to exist between the University and the third party which specifies what processing the third party is authorised to undertake on behalf of the University and action the third party must take in the event of a security breach or a subject access request.

The Data Controller and Data Protection Officer

The University is the data controller under the Act and GDPR and the University Council is therefore ultimately responsible for implementation. However, day to day matters will be dealt with by the University designated Data Protection Officer, Vicki Heath, Legal & Compliance.

Compliance

Compliance with the Act and the GDPR is the responsibility of all members of the University and any breach of the Data Protection Policy may lead to disciplinary action being taken, or access to University facilities being withdrawn, or even a criminal prosecution by third parties. 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.