Data Protection Policy
Version 3.0
Effective from January 2020

Contents

Introduction

The University has a wide range of functions as an organisation; ranging from research and education, legal services and human resources. Almost all of its functions require the University to use data about living individuals in order to deliver them.

In order to use personal data, the University must comply with all relevant UK data protection legislation. As of 25th May 2018, this means the **General Data Protection Regulation (GDPR**) and the **Data Protection Act 2018 (DPA)**.

Whilst the introduction of the GDPR strengthens a number of areas of data protection, it can be seen as an extension of data protection rather than a revolution of how data must be used by organisations. The change to the law does not mean tearing everything up and starting again but it may mean further measures need to be taken to protect the personal data that the University uses.

1. Purpose & Scope

The University's Data Protection Policy is produced for a number of key purposes and is intended to be read by staff that handle personal data.

- It gives an overview of how data protection applies to all University staff. It tells staff how data protection applies to their day to day work and areas of data protection that they must be aware of.
- This policy gives practical advice to staff about what to do in specific situations, such as receiving a rights request, discovering a potential data breach and to comply with data protection when handling personal data.
- It makes staff aware of the University's commitment to data protection compliance and tells staff where to obtain further advice and information where necessary.
- This policy has been approved by the University's Information Governance Committee. Any breach of this policy will be taken seriously and may result in disciplinary proceedings.
- Any individual who considers that the policy has not been followed in respect of their personal data should raise the matter with the University Data Protection Officer, 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 immediately to the Data Protection Officer.

2. Data Protection Definitions

2.1 Personal data

Personal data is *information that either on its own, or when combined with other information, can identify a living individual.*

This can include (but is not limited to):

Names, addresses, student and staff ID numbers, dates of birth, photographs, social media handles, video footage, emails and WhatsApp messages.

Personal data has a very wide definition and can include descriptions, personal opinions and intentions. *For example, a man sat with a group of women can be identified by the fact that he is male. This statement alone is enough to identify him and therefore is personal data.*

The main types of personal data that the University uses are: Staff Data, Student Data (prospective, current and alumni) and Research Data.

2.2 Special Category Data

Certain types of personal data are deemed more sensitive than others. Personal data that falls into the following categories is called special category data. These categories of data require extra safeguards to be met when they are used.

Personal data that fall into the special categories are related to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetic data
- Biometric data
- Health data (either physical or mental health)
- Sex life or sexual orientation

2.3 Processing

Data protection legislation refers to the processing of personal data. *Processing simply means any use of personal data.* This can range from collecting it to sharing it, from amending it to deleting it.

2.4 Data Controller

An organisation or individual that decides how and why personal data is collected and used is called a Data Controller. Data Controllers are responsible for all areas of complying with data protection legislation and must also register with the Information Commissioner's Office (the regulator for information law).

The University's registration number is **Z6390975**.

3. The Principles of Data Protection

Data protection is a principle-based law, meaning that there are a number of guiding principles that the University must meet. These principles guide how we handle personal data and each principle must be met completely.

The data protection principles state that personal data shall be:

- Processed fairly, lawfully and in a transparent way.
- 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.
- Kept for no longer than is necessary.
- Kept secure.

The GDPR also includes a responsibility for the University to document and demonstrate how it complies with the law.

3.1 How the Principles Apply

The University has a responsibility to ensure that its staff are aware of the data protection principles and ensure they are followed at all times. Data protection applies to all types of personal data held by the University, whether they are paper based or electronic.

3.1.1 Principle 1 – Fair, Lawful and Transparent

Transparent

When using personal data, the University must be open and clear about what the data will be used for and how it will be used. The GDPR requires the University to provide a wide range of information to the person whose data we are using. This is done through Privacy Notices (sometimes called Privacy Policies).

A good Privacy Notice must be clearly and plainly written, be communicated to the person whose data we are collecting at the earliest possible opportunity and contain the following information: -

- The name and contact details of the organisation that will own their data (usually the University).
- The purposes we will use their personal data for.
- The University's lawful basis (see more below) for using the personal data.
- How the individual can change their mind or opt-out of their data being used.
- The types of personal data we will use about them (e.g. – their name, their date of birth and their nationality).
- Who we will share the information with and/or who within the University will be able to access it.
- How long we will keep the data for.
- How their data is stored securely.
- Whether their data will be transferred abroad.
- Whether their data will be used to make any automated decisions about them or used to profile them.
- What rights the individual has over the use of their data.
- How to complain about the use of their data, both internally to the University's Data Protection Officer or to the Information Commissioner's Office.

Practical Tip
Ensure all application forms, surveys and contact forms have an accompanying Privacy Notice, whether they are online or in paper form. Current University Privacy Notices are available on the University website.

Fair and Lawful

The University must always ensure its use of personal data is both fair and lawful.

Fair means that we must consider whether our use of personal data may affect individuals and consider any adverse impact on them. It also means that we are open and honest with them through our Privacy Notices about how their data is used.

Lawful means that the University does not use personal data for any unlawful purposes and that personal data is not used to break either data protection or any other law of the land. This could include a breach of confidence, the Human Rights Act or copyright.

Lawful also requires the University to identify a legal basis within the GDPR for its use of personal data. The GDPR contains six lawful bases. One of them must be applied to every function that requires the use of personal data.

The lawful bases are:

- **Consent** – The individual has given their clear agreement for the University to use their data for the purpose.
- **Contract** – The use of personal data is necessary for a contract we have with the individual or steps we are taking to enter into a contract with them. This is the most common legal basis for HR activity.
- **Legal Obligation** – The use of personal data is necessary for the University to comply with the law. This could be a statutory obligation or a court order.
- **Vital Interests** – The use of personal data is necessary to protect someone's life. This is usually a life or death situation.
- **Public Task** – The use of personal data is necessary to provide a task in the public interest or is in line with a power in law that University has. This is often used for research purposes.
- **Legitimate Interests** – The use of personal data is necessary to support the legitimate interests of the University or a third party. This condition also states that the University must not use information in this way if it will compromise the rights or freedoms of the person who the data is about.

Practical Tip
The University **must** decide a legal basis for its use of personal data for each of its functions. In some cases, this will be clear but others may be more difficult to decide. If you need help with deciding a legal basis, please contact the Data Protection Officer for advice.

3.1.2 Principle 2 – Collected for a Specific Purpose

The University must ensure that it collects personal data for clear, appropriate and legitimate purposes. Collecting personal data "just in case" for future reference is not compliant with the legislation.

Through our Privacy Notices we must communicate our purposes to individuals when we collect their data in a clear way. If you feel the need to hide a purpose from the individual, perhaps we shouldn't be collecting personal data for it.

Whilst the GDPR state the University must only use personal data for the purposes we specify, it may also re-use that data for compatible purposes. For example, we may collect personal data to monitor attendance at lectures. It would be compatible purpose to re-use that data to produce statistics to monitor attendance records against educational attainment. Where you are re-using personal data for a new purpose, the Data Protection Officer can advise if this is appropriate.

Practical Tip

Ensure that you have fully identified your purposes for using personal data and that all of them are communicated in your Privacy Notices.

3.1.3 Principle 3 – Adequate, Relevant and Limited to what is Necessary

The University must only use, collect or share personal data in a proportionate way. This means that it should collect what it needs to complete its purposes but nothing more than that.

For example, if we need to collect a student's name and address for the purpose, that is all we should collect. It might be nice to know their eye colour and their favourite band, but if we don't *need* it to complete the purpose, we shouldn't collect it.

Practical Tip

Periodically review the personal data you collect and how it is collected to ensure that you are only collecting what is necessary.

3.1.4 Principle 4 – Accurate and Up to Date

Personal data must be accurate and up to date. Inaccurate information is one of the key contributors to data protection incidents. Without accurate information, the University cannot complete a wide range of key University functions. For example, if we didn't hold accurate contact details for a student, we wouldn't be able to get in touch with them.

Collecting inaccurate data is an automatic breach of the GDPR. Where inaccuracies are identified, they must be rectified as soon as possible and as many steps taken as possible to ensure the correct information is updated on University systems.

Practical Tips

a) Always double-check what you enter into University systems and emails. It is easy to press the wrong key and create an inaccurate record or send an email to the wrong person. Always take a moment to check and ensure you have entered all information accurately when you finish typing.
b) Ask a colleague to double-check you have entered the correct name and address on any documents you send in the post. It only takes thirty seconds and can save a lot of problems in the long term.
c) When collecting new information about an individual, ensure that their record is kept up to date so that all staff that have access to the data can view the most current details.

3.1.5 Principle 5 – Kept No Longer Than Is Necessary

Personal data must only be kept for a specific period of time. This time period will vary depending on what purpose the personal data is collected for. The University's Retention Schedule details how long personal data should be kept for each function.

Some computer systems will automatically delete data when it reaches its deletion date. The majority will not. This means that you need to be proactive in reviewing what data is held within your teams and how long it needs to be kept for.

Where possible, teams are encouraged to use anonymisation or pseudonymisation techniques to depersonalise the data they hold. This will provide a greater level of GDPR compliance.

Personal data held for research and archiving purposes is largely exempt from retention, where this is the only purpose for holding it. However, this data cannot be re-used for another purpose or to make decisions that affect the individuals the data is about.

Records Management is able to provide guidance and advice around retention periods.

Practical Tip
Regularly review the personal data that your team holds and assess whether it is still required or whether its retention period has expired.

3.1.6 Principle 6 – Stored Securely

The GDPR states that the University must take appropriate "technical and organisational" measures to keep the personal data that we hold in a secure way. This does not only apply to personal data held electronically, it also applies to physical documents that hold personal data.

We must ensure that our systems have confidentiality, integrity and availability, and that they can be restored in the event of a system outage.

Keeping personal data secure can be done in a range of ways, often a combination of technical and organisational measures will be used to provide the maximum level of security.

Some examples of technical measures

- Firewalls.
- Anti-virus software.
- Encrypted devices.
- Password protection.
- Access based controls to systems.
- Confidential waste bins.
- Regulated access to University buildings.

Some examples of organisational measures

- Policies and procedures that give staff information about handling personal data.
- Data protection training.
- Increased staff awareness and appropriate culture around data protection.
- Guidance notes for staff.
- Written contracts with system providers and other organisations that hold personal data on behalf of the University.
- Periodic audits and reviews of data protection practices.

Practical Tips

a) Assess the measures your team has in place to keep personal data secure. Are they consistent? Are they robust? Are you finding any common errors in your practices that lead to data protection incidents such as lost or mis-sent information? If so, contact the Data Protection Officer for advice.

b) Ensure that staff annually review policies and procedures around their use of personal data. If a process changes, ensure it is documented so that all staff are able to avoid making errors.

c) If something goes wrong, report it. Inform your line manager in the first instance and then the Data Protection Officer. If an incident is serious, it must be reported within 72 hours of discovery. The Data Protection Officer will be able to offer practical advice about how to mitigate the risk of any data protection incident.

4. The Rights of the Individual

Under data protection legislation, all individuals have a range of rights they can use to understand how their personal data is used by the University or exert an amount of control over how it is used.

One of the rights is **the right to be informed**. This is covered in the Fair and Transparent section (3.1.1).

The Rights include:

- The Right of access (often called Subject Access Requests) – an individual has a right to see a copy of the personal data held about them by the University and find out what it is used for.
- The Right of rectification – an individual can request that inaccurate information held about them is either rectified or deleted.
- The Right of erasure (Right to be forgotten) – an individual may ask for their personal data to be deleted by the University.
- The Right of restriction – an individual may ask that the use of their data is restricted whilst a complaint regarding its use is dealt with.
- The Right of data portability – an individual may ask for certain types of their data to be transferred directly to another organisation.
- The Right to object – an individual has the right to stop their personal data being used for certain purposes. This applies to direct marketing through calls and emails.
- Rights over automated decision making and profiling – an individual has the right to stop automated decisions being made about them and ask for human intervention instead. *The University does not currently make any automated decisions using personal data.*

Although the rights of the individual are a key foundation of how data protection works, the rights are not absolute. For example, the Right of Access is subject to numerous exemptions and the other rights only apply in certain situations and to certain types of data.

General Rules Around Rights Requests

- A request can be made verbally or in writing.
- The University will need to identify the person making the request and verify who they are.
- The University must respond to rights requests within **30 days** of receipt.
- The University cannot charge the individual for their response.

What to do if you receive a Rights Request

Rights requests are generally received directly by Legal & Governance. However, they can be made to any University department. It is important that all staff know what to do if they receive a request and act quickly so the response is not delayed.

- Rights requests must be forwarded immediately to legal@liverpool.ac.uk
- Rights requests will often not state they are a Rights request specifically. They can come in as part of conversations with students, staff or members of the public. Often, they come in as part of complaints.
- The individual does not have to state that they *"wish to use their right of access under the GDPR". If any individual asks* to see the information the University holds about them, this is Subject Access Request.
- If you are unsure whether the correspondence you have received is a Rights Request, send it the Legal & Governance Team anyway for assessment and completion.

5. Data Protection Incidents and Breaches

It is important that all staff are aware of data protection and what to do in the event of a data breach. Under 4.1.6 Principle 6, examples of technical and organisational measures used to keep personal data secure were detailed. It is important that the University has as many of these measures in place as possible.

When investigating a data protection issue, it is important that a clear distinction is made between an "incident" and a "breach".

An **incident** is the event that happens, where something has gone wrong.

For example, a member of staff leaves their laptop on a train. The laptop contains exam results and student details.

A **breach** is where the University hasn't used enough technical or organisational measures to stop the incident from happening.

For example, a member of staff leaves their laptop on a train. The laptop contains exam results and student details. The University has not taken steps to encrypt the laptop meaning it can be accessed by anyone.

The Information Commissioner's Office is the regulator for data protection in the UK and has the power to levy fines and other enforcement measures on organisations that suffer serious breaches. These fines are for measures that aren't taken to stop incidents from happening.

To complete the example above, the University would be fined by the ICO because they hadn't taken measures to encrypt their equipment, not because a member of staff left the laptop on the train.

This example shows that the ICO are concerned with how the University looks after personal data, rather than the individual involved. Staff and students are encouraged to report incidents as soon as they happen to that they can be mitigated for the benefit of the University as a whole.

Further examples of data protection incidents include (but are not limited to):

- Emails sent to the wrong recipients.
- Letters sent to the wrong address.
- Documents lost or misplaced.
- Information collected from individuals without a privacy notice.
- Inaccurate information entered onto University systems.

Staff Responsibilities around data protection incidents

- Regularly review policies, procedures and security measures around how data is stored, collected and shared. If any gaps are identified, inform the Data Protection Officer and ask for advice. This can help prevent future incidents.
- Report any incident, no matter how minor you believe it to be, to the Data Protection Officer through the Legal & Governance mailbox. Minor incidents can not only escalate but can also be used to identify trends in weaknesses in the University's data protection approach.
- Handle personal data with respect at all times. All staff should handle personal data responsibly and take professional pride in ensuring its security and integrity.

6. Responsibilities under this Policy

Senior Information Risk Owner

- To oversee and promote an appropriate data protection culture within the University.
- To provide a view on contentious data protection issues raised within the University.

Data Protection Officer

- To advise individuals within the University over the use of personal data and compliance with the law.

- To oversee compliance measures and ensure the University complies with the law as far as possible.
- To liaise with the Information Commissioner's Office over serious data breaches.
- To oversee and promote an appropriate data protection culture within the University.

Individual Members of Staff

- To handle personal data in a responsible and appropriate way.
- To report data protection incidents and risks to the University's data protection compliance to the Data Protection Officer as soon as possible.
- To forward Rights requests to the Legal & Governance Team as soon as possible upon receipt.
- To use University systems and communications tools (including email) in a professional manner at all times.

7. Policy Compliance

Failure to comply with this Policy and associated guidance in protecting University information (or that entrusted to us by a third party) puts the University at risk of reputational damage as well as a breach of legal and regulatory requirement. It may also lead to disciplinary action in accordance with the relevant Disciplinary Policy (staff or student) or misconduct investigation in accordance with relevant Misconduct Policy.

Where staff members deliberately or maliciously remove, destroy or sell personal data belonging to the University, the incident will be reported to the Information Commissioner's Office and dealt with through the University's disciplinary process.

The DPA contains numerous criminal offences for deliberate misuse of personal data. Where a member of staff has committed an offence of this nature, the University will pursue this offence as far as possible.

8. Data Protection Tips for Staff

Using personal data in a safe and secure way does not need to be complicated. All staff are reminded to follow the points below and refer to this policy first or ask for advice from the Data Protection Officer if they are unsure of how to proceed.

- Always lock your screen when you leave your desk. This avoids leaving your systems open to access and also stops those nearby reading any personal data you may have left onscreen.
- Clear documents away at the end of the day or when leaving your desk. This stops people who are walking past your desk from reading things they shouldn't.
- Always check for ID when holding doors open for people. It is everyone's responsibility to ensure the security of University buildings and make sure only authorised staff have access to them.
- Double check when entering information into University systems. Taking the time to check addresses and phone numbers is a vital part of data handling.
- Double check addresses when sending emails. It is easy to mistype or click the wrong name on Outlook. Once the email has gone, it cannot be retrieved. Take the time to get the recipient right before you press send.
- When taking information out of the office, think about the most appropriate way to do so. University tablets and laptops are encrypted and difficult to access if they are lost. Paper documents are not as secure as they can be read by anyone who finds them.
- If you don't need to print something, don't.
- If you are regularly sending personal information to organisations outside of the University, ensure that you verify who you are contacting and password protect the document if necessary.
- Where possible avoid using names and other identifiers in email subject headings and meeting/calendar requests.
- Take care when working from home. Your family members don't have a right to see the information you use for work.
- Don't leave equipment or documents in your car overnight if you need to take them home. You wouldn't leave your own laptop on the front seat of your car, so don't leave your work one one there either.

Using University Systems

- Just because you have access to a system, this does not mean you have the right to access all of the information on it. Access is on a "need to know" basis.
- "Curiosity" checks are not permitted. You must have a genuine, legitimate work purpose to access information
- Never share passwords. If a colleague forgets their password, they need to have it reset by IT. Do not let them access a system under your username.
- Any information you access on a system will be logged. Do not let colleagues use your computer to retrieve information and do not undertake requests on their behalf.
- Always be professional when using University systems. Do not input anything derogatory, inappropriate or rude about individuals.

9. Who to Contact

If you need further advice about data protection, please see the staff intranet pages for guidance and processes. These pages will be updated periodically with FAQs and other documents. Please contact the Data Protection Officer if you have specific questions.

Dan Howarth
Data Protection Officer
Legal & Governance
Foundation Building
University of Liverpool
Brownlow Hill
Liverpool L69 7ZX

Tel: +44(0) 151 794 2148
Email: daniel.howarth@liverpool.ac.uk & legal@liverpool.ac.uk

10. Policy Document Control

Policy Version Control			
Author	**Summary of changes**	**Version**	**Authorised & Date**
Data Protection Officer	Revision of policy	V3.0	IGC: 07/01/2020
Director of Legal & Governance	Reviewed January 2017	V2.0	
Director of Legal Services	Produced November 2008	V1.0	
Policy Management & Responsibilities			
Owner (usually HoD)	This policy is owned by the Director of Legal & Governance on behalf of the Information Governance Committee. The Director of Legal & Governance has the authority to issue and communicate policy on legal and statutory compliance including related priorities. The Director of Legal & Governance has delegated responsibility for the day to day management, implementation and communication of the Policy to the Data Protection Officer.		
Policy Review			
Review due:	Annually by January 2021		
Document Location:	Legal & Governance website www.liverpool.ac.uk/legal		

	University Policy Repository (under development)
** The Owner & Author are responsible for publicising this policy document.**	