Data Protection Policy

Version Number 4.0

Effective from May 2024, updated October 2024

Author: Director of Legal Services

Legal and Compliance Services

Table of Contents

1.0 Purpose

The University of Salford ("the University") takes its responsibilities with regards to the requirement of Data Protection very seriously. This policy will set out:

- how the University complies with the UK General Data Protection Regulation ("UK GDPR") principles
- responsibilities and accountabilities for data protection
- our approach to privacy by design and by default
- how the University manages data protection and privacy risks, in particular potential or actual personal data breaches.

The Data Protection Act 2018 (DPA18) and the UK GDPR (together "the Regulations") are designed to protect personal data and uphold the rights and freedoms of living persons. The Regulations are laws that govern how organisations process personal data.
The University processes (holds, obtains, records, uses, and shares) large amounts of personal data (personal data is defined in the UK GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person") relating to its current, former and future staff and students; research, academic and industry contacts; contractors, visitors and users of all University services. The University is obliged to meet an individual's reasonable expectations of privacy by complying with existing data protection and privacy law.

The University takes its responsibilities seriously and is committed to compliance with the Regulations, alongside continuous improvements towards improved adherence. The purpose of this document is to set out the approach to data protection at the University in order to protect personal data as well as the reputation and security of the University.

2.0 Scope and Registration

The University is registered with the Information Commissioner's Office ('ICO') under registration number Z469563X

This policy applies to all personal data[1] and special category data[2] processed (processing means the use of any personal data) or controlled by the University and on its behalf, regardless of where the information is located.

All staff, students and those acting on the University's behalf who process personal data must be aware of and comply with this Data Protection Policy when carrying out their function.

[1] Personal data is data which can identify living individuals. This includes names, contract details, statistical information and images.
[2] Special categories of data include information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life or sexual orientation, or genetic or biometric data used to uniquely identify an individual

3.0 Data Protection Principles

The Regulations set out seven key principles that organisations must follow and meet. These principles lie at the heart of the approach to processing personal data (including through the University's processes for subject access requests – SARs). They are not hard and fast rules, but rather embody the spirit of the general data protection regime – as such, there are very limited exceptions.

3.1 Lawfulness, fairness and transparency

The University must have a legal basis under the Regulations for collecting and using personal data and that data must not be used to contravene any laws. This is known as a lawful basis. The University has identified the lawful bases it relies on to collect and process personal data. The University ensures that we are open and clear with individuals about how their data will be used via Privacy Notices / Privacy Policies which are made available to data subjects.

3.2 Purpose limitation

The University ensures that the purposes of processing personal data are set out from the beginning and provides individuals with information on how their personal data will be used. If the University plans to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, it will ensure that the new use is fair, lawful, transparent and compatible with the original purpose.

3.3 Data minimisation

The University ensures that the personal data held is adequate, relevant and limited to what is necessary. The University identifies the minimum amount of personal data needed to fulfil its purpose.

3.4 Accuracy

The University takes reasonable steps to ensure that the personal data held is accurate and up to date. There is careful consideration of any challenges to the accuracy of information.

Any incomplete or inaccurate data will normally be permanently deleted or rectified immediately.

3.5 Storage limitation

The University ensures that personal data is not kept for longer than is necessary. The University's retention schedule outlines the retention periods for categories of information. Staff should be aware of the retention schedules for the information that they process and ensure that information is not kept for longer than is necessary. Where possible departments should audit their systems with the retention schedule to make sure that their processes and procedures are adhering to the policy.

If possible, it is recommended that any data collected is anonymised or pseudonymised to depersonalise the data held. This will provide a greater level of security.

3.6 Integrity and confidentiality (security)

The Regulations require that there be appropriate technical and organisational security measures in place to protect personal data. The University policies, culture, organisational structures and operating environment promote the confidentiality, integrity and availability of the University's information assets throughout their lifecycle from beginning, through use to end of use.

The University will regularly evaluate the effectiveness of its safeguards in place to ensure security when processing personal data.

3.7 Accountability

The University has appropriate measures and records in place to be able to demonstrate compliance with the accountability principle. This includes recording decisions relating to data sharing, implementing data protection policies and procedures and taking a "data protection by design" approach. The University documents its records of processing.

4.0 Roles and Responsibilities

4.1 Roles

a. Data Protection Officer - The Data Protection Officer ("DPO") is responsible for monitoring internal compliance with data protection legislation. They monitor compliance with the Regulations, advises on data protection obligations and acts as a contact point for the Information Commissioner's Office (ICO). The Data Protection Officer also ensures that communication is made with each school or professional service through regularly held Data Protection working groups.
b. Information Governance Team – A team within the Legal and Compliance Services team which assists the DPO in the performance of their functions including providing data protection advice, responding to subject access requests, etc..
c. Data Protection Working Group (comprised of Data Champions) – see paragraph 8.1.
d. Privacy Forum – see paragraph 8.1.

4.2 All staff (including temporary, contractors and volunteers) and students are responsible for:

- adhering to this policy together with other supporting polices such as the IT Acceptable Use and Information Security Policy
- ensuring that appropriate technical and practical measures are taken to safeguard personal data held from accidental or deliberate disclosure, loss, damage or destruction;
- checking that any personal data that they provide to the University is accurate and up to date;

- being mindful of the fact that individuals have the right to see their 'personal data' (and this may include for example information received from prospective students or staff written in connection with an application to the University or any comments written about them in emails). They should be mindful when recording comments or other data about individuals which they would not be comfortable with the individual seeing, either in emails or elsewhere.
- immediately reporting the matter to their line manager and bringing it to the attention of the Data Protection Officer, if they find any lost or discarded data which they believe contains personal data, (for example, may include a memory stick)
- informing the University of any changes to their personal information that they have provided, e.g. change 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;
- ensuring that they only process personal data where they have a lawful basis to do so;
- sharing information only where there is a lawful basis to do so;
- complying and handling data in accordance with the privacy policies;
- where possible holding personal data anonymously to improve security;
- completing data protection impact assessments on all new data sharing projects and submit to the foi@salford.ac.uk inbox;
- referring all requests made under data subject access request or freedom of information requests to the foi@salford.ac.uk inbox for the compliance team to review and respond;
- seeking advice or clarification if they are ever unsure of holding / disclosing personal data;
- completing training on data protection/GDPR set by the University;

Everybody should immediately report any actual or suspected misuse, unauthorised disclosure or exposure of personal data, near misses, or working practices to their line manager, principal investigator, other research supervisor or the Information Governance Team as appropriate; not retain data for longer than is necessary for the purposes for which it was collected. Personal data must be deleted or destroyed in accordance with the University's Data Retention Policy. Staff that involve students within projects which involve the processing of personal data, must ensure that those students are trained on Data Protection/GDPR, that they are aware of the Regulations and Data Protection Principles. Any staff or student who breach this policy could face sanctions as set out under the University's policies.

The University exercises overall control over how and why personal data is processed in order to comply with data protection law.[3]

[3] Processing includes holding, storing, deleting, sharing, and using data in any way.

5.0 Rights of data subjects

A data subject is any person whose personal data is being collected, held or processed. Data subjects have a number of rights in relation to the way we process their personal data. These include:
the right to be informed about the collection and use of their personal data;

- the right of access to their personal data that the University holds (Subject Access Request ('SAR'))
- the right to rectification: to have inaccurate personal data rectified, or completed, if it is incomplete;
- the right to erasure, also known as the right to be forgotten;
- the right to restrict processing;
- the right to data portability;
- the right to object to the processing of their personal data (in certain circumstances);
- rights in relation to automated decision making and profiling;
- the right to be notified of a personal data breach which is likely to result in a risk to their rights;
- the right to make a complaint to the ICO.
- details of any relevant safeguards where personal data is transferred outside of the UK/EEA.

The rights above are not absolute and any request from an individual should be referred to the Information Governance team.

The University ensures procedures in place for the assessment, management and monitoring of all individual rights requests. All individual rights requests are managed in line with the Subject Access Policy and Individual Rights Policy.

6.0 Data Sharing

6.1 Internal sharing

Personal data may only be shared internally if it is necessary to achieve the purposes for which it was collected for, or other lawful purpose.

Guidance for best practice would include:

- Only the minimum amount of data is being shared and that is of appropriate quality;
- Taking reasonable steps to ensure the data is accurate;
- Controlling access to shared drives;
- Using secure/password protected attachments within emails rather than including the data within the email;
- Checking recipients' email addresses are correct.

If there are any concerns or queries, the individual aiming to share the data should consult their line manager or the Information Governance team at foi@salford.ac.uk.

6.2 External sharing

e. Routine sharing: personal data can only be shared with third parties if there is a lawful basis to do so. For routine sharing where there is no contract in place, a data sharing agreement should be approved by the business owner, before any sharing takes place. The agreement needs to outline the purposes for sharing and the expectations for each party's processing of the data.

f. Ad hoc requests to share**:** before sharing data, it must be established that there is a lawful basis to share the data. This entails checking the identity of the person making the request, ensuring there is a secure means of sharing the data, only sharing the minimum data required, and recording the decision to share and associated and actions. If there are any concerns or queries, the individual aiming to share the data should consult their line manager, a DP Champion or the Information Governance team at foi@salford.ac.uk.

6.3 International Transfers

The GDPR applies primarily to organisations located in the European Economic Area. UK GDPR mirrors GDPR and has been UK law since January 2021. If personal data is transferred outside the UK or EEA, there is a risk that individuals will lose the protection of the GDPR / UK GDPR. As such, the GDPR / UK GDPR restricts the transfer of personal data outside the EEA or the UK as applicable unless individual rights and freedoms in respect of personal data are protected in another way as set out in the GDPR Article 46, e.g. by using standard contract clauses and the UK addendum.

An international Data Transfer Risk Assessment is needed for transfers of qualifying data outside the UK, EEA or a country recognized as adequate by the UK Government. Advice must be taken in this regard from the Information Governance team.

7.0 Data Retention

Personal data must be kept for no longer than is necessary for the purpose for which it is processed. The University has a Data Retention Schedule detailing how long different types of records should be retained. Some timescales are legal requirements whilst others are according to the needs of the school/professional service or University.

If there are any concerns or queries, the individual aiming to share the data should consult their line manager the DP Champion for their area or the Information Governance team at foi@salford.ac.uk.

8.0 Privacy by design and by default

Data protection is the responsibility of everyone within the University, and effective planning and the adoption of good behaviours prevents many issues arising. By implementing the

following initiatives, we ensure the privacy of every data subject remains a key priority in decision making and in everyday ways of working.

8.1 Privacy Forum and Data Protection Working Group

The Data Protection Working Group is held monthly and attended by the Data Protection Manager and Data Protection Champions. It discusses all issues relating to data privacy, protection and security, and information governance.

The Privacy Forum takes place bi-annually and is a meeting to formally consider and report on all Data Protection issues.

8.2 Training

All staff employed by the University, whether permanent or temporary, must complete data protection training within one month of their start date. Completion of data protection training is monitored and reported as appropriate within the University.

Staff are encouraged to use their training to make sure all systems and processes are reviewed regularly to make sure that they comply with this policy.

8.3 Contractual Requirements of Third Parties

Standard contractual terms and conditions should be in place detailing the obligations for both parties. The third party must provide sufficient guarantees on how it will process and protect the data before any data is shared. Third parties processing personal data on behalf of the University are required to provide assurance that staff have received appropriate training.
A template agreement for data processors can be found here.

Where data will be processed by a third country outside of the EEA and not defined as having adequate levels of protection by the EU, additional standard contractual clauses are required.

8.4 Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment (DPIA) is a process to help to identify and minimise the data protection risks of a project and should be seen as a living document throughout your project.

At the start of any project planning or initiative, the DPIA triage questions should be completed. If a DPIA is required, then one should be completed as soon as possible and updated throughout the lifetime of the project. A DPIA should be used to consider potential harm to individuals, the University and other organisations if personal data is shared inappropriately and/or without consent. A DPIA is a living document to be reviewed and the risk assessment element to be amended as necessary. All DPIAs are reviewed by the legal and information governance team and this process will ensure that the University only processes personal data which is necessary for the purpose of the project.

If the project involves the transfer of personal data outside of the UK/EEA, then an international data transfer must be completed prior to the commencement of any project to make sure the team have or will implement relevant safeguarding measures.

Full detail of the Data Protection Impact Assessment procedure can be found on the Data Protection & Information Governance hub page.

9.0 If Things Go Wrong

9.1 Risk Management

Risks are managed in line with the University's Risk Management Policy and are reviewed and monitored by the Data Protection Working Group and bi-annual Privacy Forum.

The Information Governance team provide an annual update to the University Leadership Team on figures and response data for Freedom of Information, Subject Access Requests, Third Party Requests and Data Protection Breaches.

9.2 Data Protection Breaches

The Data Breach Procedure is in place for the identification, reporting and management of near misses, incidents and serious breaches. As soon as a breach has occurred or discovered, immediate remedial steps should be taken along with a formal report to the Data Protection Manager via ServiceNow.

The DP Manager will grade the breach between 0 – 5 in severity, with 5 being a significant breach. The grading enables the appropriate levels of contact, actions, response and investigation. Data Protection in the UK is regulated by the Information Commissioner's Officer and they have the power to issue fines and enforce any measures they deem necessary after their own independent investigation.

Full detail of the Data Protection Breach procedure can be found on the Data Protection & Information Governance hub page

10.0 Compliance

Failure to do comply with this policy could result in financial and reputational damage to the University and lead to disciplinary or legal action against the individual.

Remember: protect the University, protect individuals and protect yourself.

If any person fails to comply with this policy, the University can enforce disciplinary procedures

11.0 Support and Escalation

The Data Protection and Information Governance team offers advice and guidance in relation to all aspects of data protection and can be contacted at foi@salford.ac.uk.

12.0 Changes to this policy

We reserve the right to change this policy at any time. A staff communication email will be circulated if the policy is updated but this policy should be reviewed regularly to ensure compliance.

13.0 Related Documentation

- Privacy Notices
- ICT Acceptable Use Policy
- Information Security Policy
- Records Retention Policy
- Data Sharing Agreement
- Subject Access Request procedure
- Data Protection Impact Assessments Policy

Document Control Information			
Revision History incl. Authorisation: (most recent first)			
Author	**Summary of changes**	**Version**	**Authorised & Date**
Legal Services	Full revision and update of policy. Updates consulted via Data Protection Working Group, Approved by ULT.	V4.0	11.06.2024 Ratified by University Council, 18.10.2024
QEO	Revision of policy to incorporate policy statement, reflect GDPR and Data Protection Act 2018, add responsibilities and rights, insert information on data retention and privacy by design and default, add risk and incident management	V3.0	

Policy Management and Responsibilities:	
Owner:	This Policy is issued by the Data Protection Manager who has the authority to issue and communicate policy on Data Protection. Major policy changes will be submitted to ULT for authorisation.
Others with responsibilities (please specify):	All subjects of the Policy will be responsible for engaging with and adhering to this policy.

Author to complete formal assessment with the following advisory teams:	
Equality Analysis (E&D, HR) *Equality Assessment form*	1. *March 2020*
Legal implications (LPG)	*2. Please specify date completed and brief outcome, or N/A*
Information Governance (LPG)	*3. Throughout Review*
Student facing procedures (QEO)	*4. Please specify date completed and brief outcome, or N/A*
UKVI Compliance (Student Admin)	*5. Please specify date completed and brief outcome, or N/A*

Consultation:	
Staff Trades Unions via HR Students via USSU Relevant external bodies (specify)	1. Outcome of consultation with TU on 22.06.20; policies were felt to be appropriate. 2. USSU via Privacy Forum, March 2020. Review by Data Protection Working Group, Jan 2024

Review:	
Review due:	May 2026
Document location (webpage):	Data Protection and Information Governance hub page
Document location (link)	Data Protection & Information Governance - Home (sharepoint.com)
The owner and author are responsible for publicising this policy document.	