LUU Data Protection & Privacy Policy

What is the purpose of this document?

Leeds University Union is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It is relevant to our student members, our employees (both weekly and monthly paid), partners and contractors.

What is GDPR?

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.

Applied across Europe from 25th May 2018, implemented in the UK by the Data Protection Bill, it supersedes the UK Data Protection Act (1998) and is designed to give you more control over your personal data and to simplify the regulatory environment across the EU for data management, including how data is exported outside the EU and EEA.

In the UK, responsibility for providing guidance around compliance is handled by the Information Commissioner's Office (ICO) - https://ico.org.uk/

The GDPR applies to 'controllers' and 'processors'.

- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.

LUU - Key definitions & Contacts

Definition	Details	Comment
Data Controller	The data controller is: **Jasper Hegarty-Ditton** Director of Digital and Communications Leeds University Union j.hegarty-ditton@leeds.ac.uk	The data controller is responsible for ensuring that there is a lawful basis for processing data and that the data is processed in accordance with the relevant legislation (GDPR).
Data Processor	The data processor is: **Leeds University Union**	This includes all LUU service and departments.
Data Protection Officer (DPO)	LUU does not fulfil the criteria under GDPR under which a separate data protector officer needs to be appointed.	The data controller acts as the DPO.
Subject Access Requests	These can be made by emailing: data-subject-request@luu.org.uk	Further information is given later in this policy. **(See Individual rights)**

Principles for data processing

At LUU, we abide by the principles enshrined in GDPR, namely:

- We will process your data in a fair, lawful and transparent manner.
- We will collect relevant data for specific purposes and be explicit about how we use it.
- We will ensure and make every effort to ensure that data is accurate, and if it isn't we shall respond quickly to change it.
- We will only keep the data for as long as is necessary.
- We will process your data in a secure way, protecting against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- Where we require your explicit consent to process your data, we will ensure your choice is informed, freely given and we are transparent as to how your data will be used and how you can withdraw consent, if applicable.

Lawful bases for processing data

The GDPR sets out six lawful bases for data processing, and at least one of these must apply whenever we process personal data:

(a) **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests**: the processing is necessary to protect someone's life.

(e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

LUU processes data on several different lawful bases as determined by the data controller. To ensure we have determined the correct choices for processing, this will be reviewed regularly by our Audit & Risk committee, supplemented by verification by external legal advice if required.

To help you understand the LUU approach, we have included some examples in the table on the following page.

Lawful Base	Where it is used in LUU	Potential LUU Examples
Consent	Where we need to use your data in a new way, or to engage with external 3rd parties, we will ask for your explicit consent.	• We ask staff if they consent to share their medical data with the University of Leeds for an occupational health review. • We ask students to explicitly opt-in to marketing communications. • If we have commercial partners who want to provide offers to staff or students, for example an offer on travel insurance, we will ask for your consent to either send those offers or provide your details to those commercial partners.
Contract	When we engage in business-to-business relationships with 3rd parties, we will process any data under this lawful basis.	• We have delivered consultancy projects for the NUS in the past; processing their supplied data to provide a quotation and fulfilling the contract under the contract lawful base.
Legal obligation	Where we are required to do so under UK law, we will process data in accordance with our obligations. In the case of a legal obligation, we would not have to seek your consent to process your data.	• When we employ students and staff, we share salary details with HMRC as part of our legal reporting duties. • If we became aware of a criminal activity by a member of staff or student, we would be bound by any legal obligations to disclose that activity.
Vital interest	Vital interests are intended to cover only interests that are essential for someone's life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death.	• If you have a medical emergency with the union building, if we know anything about your medical history, we will that share with the emergency services, if you are incapable of giving that consent and it would lead to serious detriment if we didn't share the information. • If there is an accident on a club or society trip that involves physical harm to an individual, we may offer information that is beneficial to their treatment to an appropriate authority.

Public task	Not applicable	LUU is NOT defined as a public authority or body. For more information view: https://publications.parliament.uk/pa/bills/lbill/2017-2019/0074/18074.pdf
Legitimate interest	LUU uses this base for processing data in a number of instances for both staff, students and partners. It is used as you would reasonably expect to fulfil our duties in our relationship with you. As part of preparation for GDPR compliance, LUU has conducted legitimate interest assessments (LIA) during the formulation of GDPR action plans for each department.	• Effective representative democracy is a a key obligation of LUU to its members, so as part of fulfilling that obligation under our byelaws, we will communicate with students about participating and voting in student elections. • When students join a club or society, as part of fulfilling our duty of care, our Activities team will communicate relevant health and safety information, and store trip registration forms. • As you might expect for an HR function, our People team maintain personnel records so that data such as holiday leave, sickness, salary information can be record to enable LUU to fulfil its duties as an employer.

Individual rights

The GDPR provides the following rights for individuals:

1. **The right to be informed** - a key aspect of the legislation is transparency as to how and why data is collected. At LUU, where possible, we will provide privacy information at the point of collection, especially in the case where the case for processing is based your consent.

2. **The right of access** - you can request access to your personal information (commonly known as a "data subject access request").
    - At LUU we have setup a dedicated email address (**data-subject-request@luu.org.uk**) for written requests and are training staff in how to recognise and process a verbal request.
    - We will respond to requests within one month and notify you if we need further information from you to respond; whether the nature of the request mandates extending the response time and if we are refusing the request and on what grounds that refusal would be based.
    - In most case no fee will be charged.
    - However, where the request is manifestly unfounded or excessive we will charge a “reasonable fee” for the administrative costs of complying with the request, or supplying duplicate copies. This fee will depend on the nature of the request.

3. **Right of rectification** - you can request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
    - For any rectification request, please email (**data-subject-request@luu.org.uk**) and mark the email ‘Rectification Request’, providing details as to what needs to be changed.

4. **Right to erasure** - The GDPR introduces a right for individuals to have personal data erased, also known as ‘the right to be forgotten’.
    - For any right to erasure request, please email: (**data-subject-request@luu.org.uk**) and mark the email ‘Erasure request’
    - Alike the right of access, LUU will respond within one month, and notify you if there is a legitimate reason if this right isn’t applicable to your specific situation. **(See Restrictions to individual rights depending on base of processing)**

5. **Right to restrict processing**- As an alternative to submitting a right to erasure, you can request a restriction of processing data under certain circumstances such contesting the accuracy of data, the basis on which it has been collected and/or processed:
    - For any right to erasure request, please email: (**data-subject-request@luu.org.uk**) and mark the email 'Restrict processing request'
    - We will then assess your request and respond within one month

6. **Right to data portability** - The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services. The right to data portability only applies when the lawful basis for processing this information is consent - *i.e. you have supplied the data to LUU* - or for the performance of a contract; and we are carrying out the processing by automated means (ie excluding paper files).
    - For any right to data portability request, please email: (**data-subject-request@luu.org.uk**) and mark the email 'Data portability request'
    - We will then assess your request and respond within one month

7. **Right to object** - The GDPR gives you the right to object to the processing of your personal data in certain circumstances, such as an absolute right to stop your data being used for direct marketing.
    - At LUU, our approach is to offer a transparent and open approach to how and why we collect and process data, particularly in situations where we process data under the base of legitimate interest, where explicit consent is not required.
    - If you should wish to exercise your right to object, please email: (**data-subject-request@luu.org.uk**) and mark the email 'Right to object request'
    - We will then assess your request and respond within one month

8. **Right related to automated decision making including profiling** - The GDPR restricts organisations from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.
    - At LUU, we use some profiling systems as part of our staff development such as Lumina Splash to help staff understand their team's dynamic; however, these are not part of an automated decision making process.

Restrictions to individual rights depending on base of processing

The following table shows where rights are not exercisable (X) due to the lawful base of processing chosen:

	Right to erasure	Right to portability	Right to object
Consent			✖ but right to withdraw consent
Contract			✖
Legal obligation	✖	✖	✖
Vital interests		✖	✖
Public task	✖	✖	
Legitimate interests		✖	

What information does LUU hold about you?

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are 'special categories' of more sensitive personal data which require a higher level of protection.

As outlined in **'Principles for data processing'**, our approach is only to store the data we need to fulfil our relationship to you, whether you are a student, staff member, sponsor, volunteer, trustee or someone else we have a partnership with.

Each relationship will require different data collection and as part of our GDPR compliance process, we have been reviewing all our points of data collection and storage.

A detailed list of the types of information we hold is given in the following sections.

Personal data

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth
- Gender
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Transactional data (where a purchase is linked to an individual)
- Salary, annual leave, pension and benefits information
- Start date
- Location of employment or workplace
- Copy of driving licence
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history
- Performance information
- Disciplinary and grievance information
- CCTV footage and other behavioural information obtained through electronic means such as swipecard records or computer access.
- Information about your use of our information and communications systems.
- Photographs

Special categories of more sensitive data

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership
- Information about your health, including any medical condition, health and sickness records.
- Genetic information and biometric data.
- Information about criminal convictions and offences

Retention of Data

The following list identifies different types of data and the length of time they will be kept for based on the current time period required for processing and/or legal

obligations or liabilities. We periodically review our retention policies to ensure their ongoing compliance, and systems governance to ensure data is maintained or deleted according to the retention policy.

Type of data	Kept for
HR data including training records and notes of disciplinary & grievance hearings.	6 years from the end of employment
Personal data relating to volunteers and representatives	6 years from the end date
Application forms/interview notes for staff or volunteer positions.	6 months from the date of the interviews
Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy
Facts relating to redundancies where more than 20 redundancies	12 years from date of redundancies
Income tax and NI returns including correspondence with tax office	3 years after the end of the financial year to which the records relate
Statutory maternity pay records and calculations	3 years after the end of the financial year to which the records relate
Statutory sick pay records and calculations	3 years after the end of the financial year to which the records relate
Wages and salary records	6 years
Accident books, and records and reports of accidents	3 years after the date of the last entry
Health records	During employment
Health records that were reason for termination of employment, including stress related illness	3 years
Medical records kept by reason of the COSHH regulations	40 years
Club and society membership data	6 years after graduation

Advice centre casework records	6 years after the case is closed
Safeguarding incident reports	6 years
Driver's details	1 year
DBS application records	6 years
Volunteer contact details	1 year
Joblink worker records	6 years
Alumni Contact Details	Managed on an opt-in basis

Data sharing

Where we need to share data with a 3rd party as part of processing on the base of legitimate interest, we will be transparent about that sharing.

For example, if a student joins a sports club affiliated with the University of Leeds' Sports and Physical Activity organisation, then they are entitled to free access to University of Leeds sports facilities at agreed times for training and competition under the 'Cost of Sport' agreement. To enable this free access, LUU shares membership information and this sharing is clearly presented during the club registration process.

For most instances where LUU shares data with an authorised 3rd party, it is done on an informed consent basis such as:

- Asking students for consent to share their details with a potential employer as part of our JobLink service.
- Asking staff to consent for their medical records to be shared with the University of Leeds Occupational Health service.

International transfers

In our preparation for compliance, we have not identified any systems we use that process data outside the EU without relevant safeguards and a legal basis for doing so.

For example, MailChimp is a US-based platform we use for email communications for several services. It operates under the EU-U.S. Privacy Shield Framework and we have

completed their data processing agreement so we can be GDPR-compliant with respect to international data transfer and continue to use their service.

Find out more:

https://kb.mailchimp.com/accounts/management/about-mailchimp-the-eu-swiss-privacy-shield-and-the-gdpr

Security and data breaches

The GDPR requires LUU to process personal data securely. This is not a new data protection obligation. It replaces and mirrors the previous requirement to have 'appropriate technical and organisational measures' under the Data Protection Act 1998 (the 1998 Act).

At LUU we take data security and governance very seriously and continually assess and monitor our systems and systems use against robust risk assessments.

Under the GDPR there are new rules that govern the reporting of data breaches and the following sections give an overview of how to recognise and report a data breach.

What is a data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

A succinct summary is that a breach is when LUU as 'the processor' loses control of the data.

Things that wouldn't be a data breach at LUU include:

- Sharing of data between departments within LUU (the data processor) such as between managers and HR (People team).
- Sharing of data between LUU and authorised 3rd parties as part of a recognised agreement - *in both scenarios where the base for processing has been assessed as legitimate interest and where we seek consent.*

Reporting a potential data breach:

- At LUU, all suspected data breaches should be reported to the data controller. (j.hegarty-ditton@leeds.ac.uk) - please flag the email as 'Data Breach' and give details about how you believe a breach to have occured.

Feedback

If you have any requests or comments about this policy, please contact:

Jasper Hegarty-Ditton
Director of Digital and Communications
Leeds University Union
j.hegarty-ditton@leeds.ac.uk

Version Control

Version	Reference	Date	Author
v1	GDPR Launch	23/05/2018	J.Hegarty-Ditton
v2	Additions for publication	24/05/2018	J.Hegarty-Ditton