

Union Employees

Privacy Statement

Last Revised: 23rd May 2018

Introduction

LSE Students' Union ("LSESU," "we", "our" or "us") promises to respect any personal data you share with us, or that we get from other organisations and keep it safe. We aim to be clear when we collect your data and not do anything you wouldn't reasonably expect.

We understand that the current UK Data Protection Legislation, the new General Data Protection Regulations (GDPR) and the Privacy and Electronic Communications Regulations (PECR), are the main legislation we must ensure we keep to.

Facilitating our legal requirements, organisation policy and services to our Members and the LSE Community through using your personal data allows us make better decisions, communicate more efficiently and, ultimately, ensure you and others receive the services required.

Where we collect information about you from

WE COLLECT INFORMATION IN THE FOLLOWING WAYS:

- from you when you contact us directly through the application and recruitment process or during your employment/engagement;
- from other people when we check references or carry out background checks – if we do this we will inform you during the recruitment process of the exact checks that are carried out;
- any personal data we obtain from searching public records, such as the Electoral Roll, to help us verify your identity; and
- we also collect information about job-related activities through the course of your employment/engagement with us.

What personal data we collect and how we use it

Union Employees

We may collect the following categories of personal data about you:

- Personal contact details such as name, title, address, telephone number and personal email addresses
- Date of birth
- Gender
- Equal opportunities monitoring information such as ethnicity, religion, disability and sexual orientation
- Marital status and dependents
- Next of kin and emergency contact information
- National insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start and end date of employment/engagement
- Location of employment or workplace

- Recruitment information (including copies of right to work documentation, qualifications, references and other information in your CV or cover letter or otherwise provided as part of the application process)
- Copies of identification documents such as your passport and driving licence
- Employment/engagement records (including job titles, work history, working hours, training records and professional memberships)
- Compensation history
- Performance information (including appraisals)
- Disciplinary and grievance information (whether or not you are the main subject of those proceedings)
- CCTV footage and other information obtained through electronic means such as swipecard records
- Information about your use of our information and communication systems
- Photographs and video footage
- Information about your race or ethnicity, religious beliefs, sexual orientation
- Information about your health, including any medical condition, health and sickness records
- Information about criminal convictions and offences committed by you

We will mainly use your data to:

- make decisions about your recruitment and appointment
- To determine the terms on which you work/provide services for us
- To check you are legally entitled to work in the UK
- To pay you and, if you are an employee, to deduct tax and national insurance contributions
- To provide benefits to you, including pension
- To liaise with your pension provider
- To administer the contract we have with you
- For business management and planning purposes, including accounting and auditing
- To conduct performance reviews, manage performance and determine performance requirements
- To make decisions about salary reviews and compensation
- To assess your qualifications for a particular job or task, including decisions about promotions
- To decide whether and how to manage your conduct
- To gather evidence for possible grievance or disciplinary hearings (in relation to you or someone else)
- To make decisions about your continued employment or engagement
- To make arrangements for the termination of our working relationship
- For education, training and development
- To deal with legal disputes involving you or other employees, workers or contractors, including accidents at work
- For regulatory purposes
- To ascertain your fitness for work
- To manage sickness absence
- To comply with health and safety obligations
- To prevent and detect fraud or other criminal offences
- To monitor compliance with our policies and our contractual obligations, including the use of our information and communication systems to ensure compliance with our IT policies

- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- To carry out equal opportunities monitoring
- For insurance purposes
- To provide a reference upon request from another employer/third party
- To comply with employment law, immigration law, health and safety law, tax law and other laws which affect us

Under data protection legislation we are only permitted to use your personal data if we have a legal basis for doing so as set out in the data protection legislation. We rely on the following legal bases to use your information for employment related purposes:

Some personal data is classified as "special" data under data protection legislation. This includes information relating to health, racial or ethnic origin, religious or philosophical beliefs, political opinions, sex life, sexual orientation and trade union membership. This personal data is more sensitive and we need to have further justifications for collecting, storing and using this type of personal data. There are also additional restrictions on the circumstances in which we are permitted to collect and use criminal conviction data. We may process special categories of personal data and criminal conviction information in the following circumstances:

- In limited circumstances with your explicit consent, in which case we will explain the purpose for which the personal data will be used at the point where we ask for your consent.
- We will use information about your physical and mental health or disability status to comply with our legal obligations, including to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or ethnic origin, religious or philosophical beliefs, your sexual life or sexual orientation to ensure meaningful equal opportunity monitoring and reporting – the legal basis of this processing is that it is in the public interests to carry out diversity monitoring.
- We will comply with employment law obligations.

How we keep your data safe and who has access

Personal data collected and processed by us may be shared with Students' Union employees and volunteers and under strictly controlled conditions the following groups where necessary:

- Contractors
- 3rd Party Processors such as HMRC, Paycloud and Exchequer
- Service provider partners
- The London School Of Economics

When we allow access to your information, we will always have complete control of what they see, what they are allowed to do with it and how long they can see it. We do not sell or share your personal information for other organisations to use.

We undertake regular reviews of who has access to information that we hold to ensure that your information is only accessible by appropriately trained staff and contracted processors.

Some of our processors run their operations outside the European Economic Area (EEA). Although they may not be subject to same data protection laws as companies based in the UK, we will take steps to make sure they provide an adequate level of protection in accordance with UK data protection law and satisfy conditions necessary for a transfer of data outside the EEA. This includes EU Model Contract Clauses and Privacy Shields if applicable. By submitting your personal information to us you agree to this transfer, storing or processing at a location outside the EEA.

We may need to disclose your details if required to the police, regulatory bodies or legal advisors.

We will only ever share your data in other circumstances if we have your explicit and informed consent.

Keeping your information up to date

We request that LSE Staff make best attempts to ensure data held by the Students' Union is up to date and accurate. In the event of any changes to data or the discovery of any inaccuracies please update your contact information on your account at LSESU.com within the personal details section. For all other information held on our website, please contact the Activities Resource Centre.

For any other information that we may hold on you please place a Subject Access Request and a Rectification Request. These forms can be found on our data protection webpage (LSESU.com/data-protection.)

Data Retention

We try and delete data as soon as we can and we will keep your sets of data for as long as one or more of the following conditions apply:

- a) 6 years after the last financial year (our financial year ends in July) in which you were paid or reimbursed.
- b) 6 years after the end of any contract that is held between you as an individual and the Union.
- c) 5 years after your last interaction with our website / emails / Social Media.
- d) 12 months after an unsuccessful application

Understanding the detail of our data security measures

When we process your data we will have already carefully assessed the lawful basis (reason) for doing so, the parameters in which the data is processed, the length of time the data is held for, the secure storage of your data, an overview of this analysis can be accessed under the Documentation section on our data protection webpage (LSESU.com/data-protection). Where we rely upon a legitimate interest to process your data we will have completed a legitimate interest assessment.

The Students' Union operates a Data Protection, Information Security and Systems Policy which is supported by a practical handbook for our employees and a separate handbook for our volunteers. All employees and volunteers handling data are required to undertake

general data protection training, these are done on an annual basis and third parties handling data are required to provide a contract which meets the requirements of the Information Commissioner's Office.

Your Rights about Your Data

You have rights under Data Protection Legislation regarding your own personal data.

We detail all of your actionable rights on our data protection webpage ([LSESU.com/data-protection](https://www.lsesu.com/data-protection)). Depending upon the lawful basis that is required for the processing of the personal data above, some rights may or may not apply. Under our process of ensuring any rights upon request, we will inform you of what personal data is exempt from your request and the lawful basis why.

If you have any questions please send these to su.info@lse.ac.uk , and for further information see the Information Commissioner's Office Guidance (<https://ico.org.uk/for-the-public/>)

Changes to this statement

We may change this Privacy Statement from time to time. If we make any significant changes in the way we treat your personal information we will make this clear on our Website or by contacting you directly.

If you have any questions, comments or suggestions, please let us know by contacting su.info@lse.ac.uk.