DATA PROTECTION, SYSTEMS AND INFORMATION SECURITY POLICY

Introduction

The London School of Economics Students' Union is committed to the protection of the personal data of students, employees, suppliers and other individuals whom we might hold information about.

The Union acknowledges the General Data Protection Regulations and UK Data Protection Legislation and the Privacy of Electronic Communications Regulations as the primary legislation relating to data handling and processing.

To this end every individual employee, trustee, student volunteer, member, or contractor handling data collected or administered by the Union must take responsibility and due consideration for its appropriate use in line with this policy and the declared processing activities. The specific arrangements for handling, processing and administering data can be found within the Data Protection, System and Information Security Handbook.

These policies apply to all employees and volunteers, and overseen by the nominated Data Protection Officer reporting to the Union's leadership team, Audit and Risk Committee and the LSESU Trustee Board. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Union facilities being withdrawn, or even a criminal prosecution. It may also result in personal liability for the individual. Not reading or being aware of this policy document and associated handbook is not an adequate reason for non-compliance with the policy and handbooks.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

Responsibilities

Students

Students must ensure that all personal data provided to the Union is accurate and up to date, and that they have read and understood the relevant terms of conditions of engagement with the Students' Union.

For all personal information (apart from contact information) which is held on our Membership System, information which has been shared between LSE and LSESU must be updated by contacting LSE Student Services.

This is due to the way in which this data is treated in our Membership System. Contact information can be updated by logging into MSL and changing it in the Student's personal account or the Student may elect to do it themselves by logging into LSESU.com and changing the relevant data. All other personal information that is gathered by LSESU or Student Groups, the student must contact LSESU and the student groups to update.

Where a Student Opts out of Union Membership as detailed in the Data Sharing Agreement between LSESU and LSE, the Director of Membership or their nominee will block the Student ID number in MSL and contact the LSE to remove them from the Data Feed.

Suppliers and Contractors

Suppliers and contractors must ensure that all personal data provided to the Union is accurate and up to date, and that they have read and understood the relevant terms of conditions of engagement with the Students' Union. There will be further responsibilities placed upon suppliers and contractors depending if they undertake any data processing on behalf of the SU. LSESU Employees as part of their responsibilities will ensure any data processors comply with the relevant data protection legislation, and look for alternative suppliers and contractors where this compliance does not occur. This is detailed in the Data Protection, Systems and Information System Handbook.

Student volunteers

Committee members, representatives and other student volunteers may handle personal data to administer their activities and services. Students handling such data are required to have completed the data protection and information security training course prior to receiving permission to handle any personal data related to Students' Union activities and services. LSESU will make the Student Volunteer Data Protection and Information System Handbook readily available on our website and distribute as necessary to Student Volunteers at Face-to-Face training sessions.

LSESU has the right to enact restrictions and discipline upon Student Groups when Committee Members (Student Volunteers) process data without completing the training, data protection agreements, in line with this policy or in line with their handbook. When handling personal data students are required to follow the guidance set out in the Student Volunteer Data Protection and Information System Handbook including the reporting of data breaches, respecting the rights of individuals and secure processing procedures.

Further to this, LSESU asks student volunteers to sign a Data Protection Agreement to access any personal data of fellow students from LSESU's Membership System or other storage locations.

Line Managers of Volunteers must complete a Privacy Impact Assessments for the access required by Student Volunteers to personal data, before access to said personal data can be given .This must be then signed off by the Data Protection Officer to grant them access to the personal data.

Union employees (Student Staff)

The Union holds various items of personal data about its employees which are detailed in the relevant privacy notice in/at LINK. Employees must ensure that all personal data provided to the Union in the process of employment is accurate and up to date. They must ensure that changes of address etc are updated by contacting their relevant line manager to update with the Central Operations Team.

In the course of day to day working it is likely that staff will process individual personal data. Prior to handling any data, staff are required to have completed the data protection and information security training and should be follow any guidance set out in the Data Protection, System and Information Security Handbook.

Line Managers must complete a Privacy Impact Assessments for the access required by student staff to personal data, this must be signed off by the Data Protection Officer to grant them access to the personal data.

Union employees (Non-Student Staff)

The Union holds various items of personal data about its employees which are detailed in the relevant privacy notice in/at LINK. Employees must ensure that all personal data provided to the Union in the process of employment is accurate and up to date. They must ensure that changes of address etc are updated by contacting the relevant member of staff within the Central Operations Team.

In the course of day to day working it is likely that staff will process individual personal data. Prior to handling any data staff are required to have completed the data protection and information security training.

In addition to this staff must maintain a current knowledge of data processing best practice through annual refresher courses and learning available on the Information Commissioner's Office website at www.ico.org.uk. When handling personal data, staff are required to follow the guidance set out in the Data Protection, System and Information System Handbook details of which can be found at LINK.

For Employees who are implementing/decommissioning/changing processes, hardware or software they should refer to the System section further down in the policy and the relevant section in the handbook.

Union managers and Project leads

Union managers and project leads must ensure that staff handling data in the course of their roles have conducted the appropriate training, are processing data within the frameworks agreed and following the guidance set out in the Data Protection, System and Information System Handbook.

Managers are also required to conduct regular audits of their relevant spaces and IT infrastructure to identify weaknesses in information security. The maximum timeframe between audits is 18 months or when a turnover of staff in a department or team is greater than 60 % of the number of non-student staff roles currently employed over a course of less than 9 months.

Data Protection Officer

The Data Protection Officer is the currently the Chief Executive at the Union. The Data Protection Officer is responsible for:

Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws

Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.

To be the first point of contact for supervisory authorities and for individuals whose data is processed (students, employees, customers etc).

The Data Protection Officer can be a delegated authority by the Chief Executive to carry out their role with the resources required to be effective in the protection and security of the individual data the organisation handles.

The data protection officer shall be contacted via the su.info@lse.ac.uk email address in the first instance and their work email address in further instances.

Leadership Team

The Leadership Team is required to demonstrate ownership of the Union's data protection policy and to communicate its values across the Union. This accountability cannot be delegated, however operational aspects of data protection management may be delegated to other levels of management. The Leadership Team must gain assurance that these responsibilities are being fulfilled and to ensure resources are available to fulfil the requirements of this policy and associated procedures.

Trustee Board

The Trustee Board has overall accountability for the strategy of the Union and is responsible for strategic oversight of all matters related to statutory legal compliance and risk for the Union. The Trustee Board should seek assurance from the Leadership Team that effective arrangements are in place and are working through the Audit and Risk Committee.

Compliance

Respecting Individuals Rights

The General Data Protection Regulations sets out a series of rights for individuals. Union employees and volunteers planning data processing activities must record how these rights are addressed. The Data Protection, Systems and Information System Handbook details the rights and the organisation's standardised processes to meet these individual rights.

Documentation

The General Data Protection Regulations sets out a need for Data Controllers and Processors to maintain documentation on processing activities with regards to personal Data. LSESU follows a semi-centralised system where each team and department is responsible for creating and updating any required documentation. The Central Operations team will be the central holders of all documentation on behalf of the Data Protection Officer. The Data Protection, Systems and Information System Handbook details the specifics of how this works.

A Retention Schedule shall be created from the Documentation and will be held in the Shared Drive for access by all Staff. This will also be shared on the LSESU Data Protection webpage.

Processing Special Categories Of Data

The Union shall only process special categories of data linked to individuals with the consent of individuals except for where the disclosure is to preserve life, for legal purpose or is carried out in our legitimate activities with appropriate safeguards or is subject to the Data Sharing Agreement that is in place with the LSE. This data may be analysed in broad terms where no direct link to an individual can be made.

Subject Access Requests

The Data Protection, Systems and Information Security Handbook details the procedures on how subject access requests must be handled. As standard, the Union does not charge to comply with access requests and will refuse manifestly unfounded or excessive requests.

Any individual or department receiving a Subject Access Request must share this with the Data Protection Officer within 2 working days in a non-busy period and 3 working days in a busy period (including but not limited to LSESU Elections, LSESU Welcome Week). The Data Protection Officer shall confirm to the data subject receipt of the request within 3 working days from receiving the request. LSESU will instruct upon our website that where a data subject has not received confirmation from the Data Protection Officer within 5 working days, the data subject should email su.info@lse.ac.uk with the original request attached to further ensure we meet the 1 month deadline provided in the GDPR.

Lawful Data Processing

The Union shall only process data within the law. Where a lawful process has been identified; Union employees and volunteers must make a record of the lawful justification within the relevant documentation and update any privacy notices. The Data Protection, Systems and Information Security Handbook details the procedures on how to record the lawful processing justification.

Children

Union staff and volunteers shall not process data related to any individual aged under 16 without permission from the Data Protection Officer. Guidance on how data processing with Children works, see the Data Protection, Systems and Information Security Handbook

Data Breaches

The Union shall adopt processes to detect data breaches including audits and other appropriate processes. Employees and volunteers shall report and investigate data breaches as outlined in the Response Plan for Data Breaches contained within the Data Protection, Systems and Information Security Handbook.

Where an employee, volunteer, supplier or contractor discovers a data breach they must report this to the Data Protection Officer within 24 hours. The Information Commissioner's Office shall

be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals such as discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where there is a high risk to the rights and freedoms of individuals they shall be notified directly also. The reporting procedures alongside the swimming lanes are detailed in the Data Protection, Systems and Information Security Handbook.

Data Protection By Design

Employees and volunteers are required to adopt a privacy by design approach to planning data collection and processing. In addition to data collection records, Privacy Impact Assessments (PIAs) and where appropriate Legitimate Interest Assessments (LIAs) must be completed prior to any data collection or processing. Details of how to conduct PIA's and LIA's are contained within the Data Protection, Systems and Information Security Handbook.

Further information of Data Protection By Design with regards to Systems can be found further below in this policy document.

Information Security

Data Storage

Electronically stored personal data must be stored in an encrypted or password protected form to protect against unauthorised access or processing. Physical representation of data, such as paper forms, must be stored within a locked storage unit. When no longer needed, the e-copies should be deleted and any paper copies securely destroyed.

Vital records for the purposes of business continuity must be protected from loss, destruction or falsification by Union employees or staff, in accordance with statutory, regulatory, contractual, and Union Policy requirements.

The Union has 5 primary platforms for securely storing data online - Google Cloud, LSE S Drive, H Spaces, LSE Sharepoints and LSE One Drives. Staff are required to store data they handle on one of these platforms only as detailed within the Data Protection, System Procurement/Decommission/Review and Information System Handbook. Whereas Volunteers may only to store data they handle on Google Cloud or their H Space as detailed in their Handbook.

Explicit permission from line management must be obtained before removing restricted information, including personal data and confidential information from Union premises. Where possible, this should be accessed via the LSE Remote Desktop, Sharepoints, Onedrive or the Gsuite only and not downloaded onto personal devices. Restricted information processed on portable devices and media must be encrypted. The password to an encrypted device must not be stored with the device.

Third Party Contracts

Occasionally the Union may transfer data to third parties for process in line with guidance contained within the Data Protection, Systems and Information Security Handbook. Prior to data transfer a contract to ensure compliance with relevant legislation must be in place with oversight by the Data Protection Officer.

IT Systems

Employees and volunteers must undertake a data protection and Information security training to ensure sufficient security awareness. Employees and volunteers must make best attempts to protect their identity by using a strong password. Account passwords and usernames should not be shared without authorisation from organisational managers. LSESU recognises the LSE IMT policies are stringent and strong, and requires LSESU Staff and volunteers to abide by them.

Digital equipment and media containing information must be secured against theft, loss or unauthorised access when outside the Union's physical boundaries. In addition, all digital equipment and media must be disposed of securely and safely when no longer required - the Data Protection, Systems and Information Security Handbook outlines the appropriate procedures.

Systems and Processes

Definitions

Systems refer to the Electronic and non-electronic Software which are involved in operations at LSESU. Processes are the use of said systems to create meaningful output towards the strategic aims of the organisation.

System and Process Reviews

With regards to LSESU Systems, Staff teams are required to conduct regular reviews of their Systems to identify and review weaknesses in efficacy, efficiency, security and compliance with legislation. The maximum timeframe between reviews is 2 years or when a turnover of staff in a department or team is greater than 60 % of the number of non-student staff roles currently employed over a course of 1 year. Detailed requirements are set out within the Data Protection, Systems and Information Security Handbook.

LSESU recognises that due to strategic needs, systems and processes will need to change, therefore whenever a new strategy is created by the Trustee Board and the Leadership Team, a system review should follow in all teams, including when a review has occurred in the past 6 months.

System and Process Procurement

When a System is no longer fit for purpose or a new process is required, proposals may be made to procure or create a system/process. If the system/process already exists within the Union, this should looked at after the System and Process Review flowchart as stated in the handbook. LSESU will only consider electronic software and hardware that can be compliant with the relevant legislation for procurement, this includes but is not limited to Data Protection (including GDPR), and PECR.

Any new System (Software) must be approved by the relevant Director to the Team in question.

System Decommission

When a System or Process is no longer fit for purpose, proposals may be made to decommission the system/process. This decision should be taken after the System Procurement process when a balanced decision can be taken. The only time this will not occur is if the system itself is non-compliant in relevant legislation that it becomes illegal to continue to use.

Volunteers and Employees Leaving LSESU

Electronic and non-electronic systems have a large weakness in terms of those who already have access to the system. Each Team within the Union has a responsibility to ensure that all relevant passwords and access to the team's systems is removed to volunteers and employees when they leave. This should happen on the concerned person's last day. Regarding access to the LSE network and LSE IMT facilities for employees, the central operations team shall ensure as part of the leaver processes, IMT are informed and given a date to change all relevant passwords to the account to stop access after the last day. Further specifics regarding leavers are detailed in the handbook.

Policy Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Union's Leadership Team, together with reviews by the Audit and Risk Committee. The Data Protection Officer is responsible for the monitoring, revision and updating of this document every two years or sooner if the need arises.