Data Protection & Information Security Policy

Introduction

The University of York Students' Union ("the Union, "we", "us", "our") is committed to the protection of the personal data of students, employees, suppliers and other individuals whom we might hold information about.

The Union recognises the General Data Protection Regulations and the Privacy of Electronic Communications Regulations as the primary statutory responsibilities relating to data handling and processing.

To this end every individual employee, 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 at www.yusu.org/privacy-policy

These arrangements apply to all employees and volunteers, and overseen by the nominated Data Protection Officer reporting to the Union's Senior Management Team and 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breach of the data protection policy may lead to disciplinary action being taken, or access to Union facilities being withdrawn, or even a criminal prosecution.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.

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

Responsibilities

Students, suppliers and contractors

Students, 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. They must ensure that changes of address etc. are updated on the appropriate systems by contacting the relevant staff detailed in the privacy notices at www.yusu.org/privacy-policy

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 ***YUSU General Data Protection Regulations training course*** prior to receiving permission to handle any personal data related to Students' Union activities and services. When handling personal data students are required to follow the guidance set out in the ***data protection and information security handbook*** including the reporting of data breaches, respecting the rights of individuals and secure

processing procedures. Details of the training course and handbook can be found at www.yusu.org/privacy-policy

Union employees

The Union holds various items of personal data about its employees which are detailed in the relevant privacy notice at www.yusu.org/privacy-policy. 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 Human Resources.

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 ***YUSU General Data Protection Regulations training course*** In addition to this staff must maintain a current knowledge of data processing best practice through 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 and information security handbook*** details of which can be found at www.yusu.org/privacy

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 and information security handbook***. Managers are also required to conduct annual audits of their relevant spaces and IT infrastructure to identify weaknesses in information security.

Data Protection Officer

The Data Protection Officer is the Director of Finance & Resources 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 is 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 assigned the dataprotection@yusu.org email address.

Senior Management Team

The Senior Management 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 Senior Management 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.

Governing Body

The Governing Body 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 Governing Body should seek assurance from the Senior Management Team that effective arrangements are in place and are working through the appropriate delegated 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 and information security handbook*** details the rights and the organisation's standardised processes to meet these individual rights.

Processing Special Categories of Data

The Union shall only process special categories of data linked to individuals, such as health data, religious and sexual orientation, with the consent of individuals except for where the disclosure is to preserve life or for legal purpose. This data may be analysed in broad terms where no direct link to an individual can be made.

Subject Access Requests

The ***data protection 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 5 working days. The Data Protection Officer shall respond to the request within one month of initial receipt.

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 privacy notice. The ***data protection 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.

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 Cyber Incident Response Plan (CIRP) contained within the ***data protection 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 are detailed in the ***data protection 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) shall 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 and information security handbook***.

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 3 primary platforms for securely storing data online - Google Cloud, University of York secured Drives and Website. Staff and Volunteers are required to store data they handle on one of these platforms only as detailed within the ***data protection and information security handbook***.

Explicit permission from line management must be obtained before removing restricted information, including personal data and confidential information from Union premises. 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 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 ***YUSU General Data Protection Regulations training course*** 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.

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 and information security handbook*** outlines the appropriate procedures.

Policy Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Union's Senior Management Team, together with reviews by the appropriate Governing Body Committee. The Data Protection Officer is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.