Falmouth & Exeter Students' Union

Ref Number:

Board of Trustees Meeting: 22/05/2018

Confidentiality: Not confidential

Title of document: Data Protection and Information Security Policy

Submitted by: Joff Cooke

Action Required – For Approval

Document	Data Protection and Information Security Policy
Version	Version 1
Subject to Approval By	FXU Board
Approved	May 2018
Subject to review	Annually
Next review Date	May 2019
Signed	

Data Protection & Information Security Policy

Introduction
Falmouth & Exeter Students' Union ('FXU') is committed to the protection of the personal data of students, employees and other individuals whom it holds information about.

FXU recognises the General Data Protection Regulation (GDPR) and the Privacy of Electronic Communications Regulations (PECR) as the primary statutory responsibilities relating to data handling and processing.

To this end, every individual employee handling data collected or administered by FXU must take responsibility and due consideration for its appropriate use in line with this policy and the declared processing activities.

These arrangements apply to all employees and volunteers, and are overseen by FXU's senior management team and Chief Executive Officer. Any deliberate breach of this policy may lead to disciplinary action being taken, or access to the FXU's facilities being withdrawn, or even a criminal prosecution.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 Chief Executive Officer.

Why this policy exists

This Data Protection Policy is designed to ensure that FXU:
- Complies with data protection law and follows good practice
- Protects the rights of staff, members, customers and partners
- Is open about how it stores and processes individuals' personal data
- Protects itself from the risks of a data breach

Responsibilities

<u>Students/ Casual staff</u>
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 prior to receiving permission to handle any personal data related to FXU 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.

<u>FXU employees</u>
FXU holds various items of personal data about its employees which are set out in the Data Protection and Information Security Handbook.

FXU employees must ensure that all personal data they provide to FXU in the process of employment is accurate and up to date. They must ensure that changes of address etc. are updated by contacting FXU's Finance & Administration Manager.

During 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 course.

In addition, staff should 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.

FXU directors
FXU directors 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.

FXU Directors are required to conduct six monthly audits of their relevant spaces and IT infrastructure to identify weaknesses in information security.

Students, suppliers and contractors
Students, suppliers and contractors must ensure that:

- All personal data provided to FXU is accurate and up to date.
- Changes of address etc. are updated on the appropriate systems by contacting the relevant staff detailed in the privacy notices set out in the Data Protection and Information Security Handbook.

Compliance
Respecting Individuals Rights
GDPR sets out a series of rights for individuals. FXU 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 Category Data
Other than when disclosure is for the purpose of preserving life or for legal compliance, FXU shall process an individual's special category data (such as health, religious and sexual orientation), with the individual's consent only.

This data may be analysed in broad terms where no direct link to an individual can be made.

Subject Access Requests
Following receipt of a data subject access request, FXU will respond in accordance with the provisions of the GDPR.

The Data Protection and Information Security Handbook includes FXU's Data Subject Access Request procedure.

Lawful Data Processing

FXU shall process data only when a GDPR compliant basis for doing so exists.

Before processing any personal data, FXU staff and volunteers must:

- Identify a legal basis for processing.
- Make a written record of the lawful justification within the privacy notice.

The Data Protection and Information Security Handbook includes details of the process relating to recording the lawful processing justification.

Data Breaches

FXU shall adopt a process for identifying and responding to data breaches including audits and other appropriate processes. FXU staff and volunteers shall report and investigate data breaches as outlined in the Data Breach Management Procedure contained within 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

All 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 FXU employees or staff, in accordance with statutory, regulatory, contractual, and FXU Policy requirements.

FXU has the following platforms for securely storing data online – Sharepoint and the user's personal U Drive. FXU staff and volunteers must store data they handle on one of these platforms only - as detailed within the Data Protection and Information Security Handbook.

FXU recognises that from time-to-time staff and volunteers may need to remove restricted information, including personal data and confidential information, from FXU premises (for example, when travelling between campuses). In those circumstances:

- Information processed on portable devices and media must be encrypted or password protected using a password that is not stored with the device.

- It is the member of staff and/or volunteer's responsibility to taker the utmost care so as to avoid loss of data held in a physical form.

Third Party Contracts

From time-to-time, FXU enters into contracts with third parties leading to a transfer of personal data to those third parties. Prior to any data transfer, FXU staff shall ensure that FXU's contract with the third party includes provisions designed to ensure the parties' compliance with the prevailing data protection legislation.

IT systems and equipment

All FXU staff must undertake data protection and information security training to ensure sufficient security awareness.

At all times and in all locations, FXU staff and volunteers must secure digital equipment and media against theft, loss or unauthorised access.

Where possible, FXU staff should access all work-related IT systems through the VDI system only, including when working remotely.

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

Day-to-day responsibility for compliance with this Policy and its related policies and procedures rests with FXU's Chief Executive Officer and Senior Management Team.

The Chief Executive Officer is responsible for ensuring that the Policy is reviewed annually or sooner should the need arise.