INFORMATION SECURITY POLICY

Policy prepared by:	Mark Johnson, Operations Manager
Version	3.0
Policy became operational on:	15/01/2026
Next review date:	15/01/2028

Table of Contents

INTRODUCTION

This policy applies to **The University of Exeter Students' Guild** ("**the Guild**" which is a company registered in England and Wales under registration number 07217324 with a registered office at **Devonshire House, Stocker Road, Exeter, EX4 4PZ.** "**The Guild**" is the 'Controller' or sometimes the 'Processor' of personal information it processes.

All information held and processed by the Guild, in all formats, must be used and stored in a secure manner. The UK General Data Protection Regulation (UK GDPR) places an obligation on the Guild, as an organisation processing personal data, to take appropriate technical and organisational measures to protect personal data against unauthorised and unlawful processing and against accidental loss, destruction, or damage.

The Guild is mindful of the serious consequences that a breach of security can bring. There are severe sanctions which can be imposed under the UK GDPR for a personal data breach and such breaches could cause serious reputational damage which could be catastrophic to the organisation. As such, the Guild will follow the procedures set out within this policy.

SCOPE OF POLICY

This policy is applicable across the Guild and individually applies to:

- all individuals who have access to Guild information and technologies.
- all facilities, technologies and services that are used to process Guild information.
- information processed, in any format, by the Guild pursuant to its operational activities.
- internal and external processes used to process Guild information; and
- external parties that provide information processing services to the Guild.

PURPOSE OF POLICY

The Guild's objectives for information security are:

- a culture is embedded to ensure all activities consider information security.
- individuals are aware and kept informed of their information security responsibilities.
- information risks are identified, managed and mitigated to an acceptable level.
- authorised users can securely access information to perform their roles.
- facilities, technologies and services adequately balance usability and security.
- implemented security controls are pragmatic, effective and measurable.

- contractual, regulatory and legal obligations relating to information security are met; and incidents are effectively managed and resolved and learnt from to improve our control environment.

The purpose of this policy is to outline the Guild's approach to information security management and provide the guiding principles and responsibilities that ensure the Guild's information security objectives are met. It explains how the Guild will manage the security of the information it collects, uses, stores or otherwise processes, whether that information is contained within hard copy documents or electronic files. Whatever the format, the Guild recognises that information needs to be protected, and in terms of personal information, high standards need to be met.

KEEPING DESKS CLEAR

The Guild recognise the importance of ensuring that personal data is not left out on desks and is locked away when not in use, thereby preventing it from being seen or accessed by anyone not entitled to see it.

Every member of staff must ensure that:

- All personal data is locked away at the end of each day and when not in use.
- All personal data is locked away if computers are left unattended, such as when leaving the office for lunch breaks or meetings.
- The keys for the cabinets, drawers, or cupboards in which the personal data is stored are kept in a safe location out of sight.
- Documents containing personal data are not stored on open bookshelves, on top of cabinets or left on or under desks or displayed on walls. This is particularly important to ensure that staff/students who are given access to Guild offices cannot see any personal data they are not entitled to see.

Each member of Guild staff is responsible for the computer hardware they have been issued, and managers are to ensure their teams are being responsible users. No unauthorised personnel must be given access to the cupboards, cabinets, or drawers in which the personal data is stored.

The Students' Guild will only allow their visitors access to rooms in which no personal data is stored, thereby eliminating the risk of visitors accidently being given access to personal data they are not entitled to see. If visitors are given access to areas in which personal data is being stored or otherwise processed, the Guild will ensure that the personal data is securely locked away.

ACCESS TO PERSONAL INFORMATION

In terms of ensuring access to information is appropriately managed, the Students' Guild will ensure that:

- Access to records containing personal data is restricted to only those that need it for their jobs. This will ensure that nobody will have access to personal data that they are not entitled to see.
- Access to Guild offices is only provided to staff that need it. Access is either via keys or University ID cards and swipe entry. Access controls are administered by the Operations Team and once access is not required, it is revoked.
- Cleaning staff and maintenance teams are contracted through the University of Exeter and therefore already vetted so they can access Guild spaces under a lease agreement. However, it is the Guilds' responsibility to ensure confidential information is not left in sight.

PHYSICAL SECURITY

With a view to avoiding any breaches of security before they arise, Students Guild staff will be alert to potential issues and will ensure that:

- They report suspicious activity.
- Visitors and guests do not have access to any personal information they are not entitled to see.

To ensure the risk of a personal data breach is minimised, the Guild will ensure that:

- A log is kept of who holds keys to the various spaces around campus. This is managed by the operations team.
- Offices that have pin pad access. Pins are only circulated to the staff that need them. Pin numbers are cycled annually.
- Offices that are accessible via card swipe, only designated staff have access.
- All issued smart phones, tablets and laptops are signed for and that is recorded in a register.
- An asset register is maintained and kept up to date and includes assets such as smart phones, laptops, and tablets. These assets can be remote wiped by the Operations department if lost or stolen.
- Staff are instructed to report all incidents or potential incidents to the Data Protection Guardian.
- Hard copy personal data no longer required is securely destroyed in line with the secure destruction and deletion procedures and the Guild's Retention Policy and Retention Schedule.

To ensure staff remain focussed on the importance of security and protection of personal data, this topic will be included within annual data protection refresher training.

ELECTRONIC SECURITY

The Students' Guild appreciate that electronic information can be put at risk from hackers or other unauthorised use if adequate measures are not taken to protect it. In order to keep electronic personal data secure, The Students' Guild will follow the steps set outlined below.

Training

The Guild recognises the value of cyber security training for their staff and will ensure that suitable training is provided, where necessary. The training will raise awareness of cyber-attacks and will cover topics such as how to avoid problems arising, how to spot a threat and what to do when a cyberattack occurs.

Cyber Attack Simulation Training

The Students' Guild regularly launch attack simulations on the organisation to evaluate the organisation's cybersecurity posture and readiness. Testing for potential vulnerabilities and ensuring current security measures are effective, the results of the tests are included in the Guild compliance dashboard which is presented to the Trustee board subcommittee. Employees who require further refresher training be directed to training material which focusses on the type of attack experienced.

Lock Computer Screens

It is good practice for staff to lock their computers when they need to leave them unattended for any length of time, such as to attend meetings, take a comfort break or a lunch break. The Guild will ensure staff lock their screens and use strong passwords or Multi Factor Recognition to access their computers again. We will also ensure that screens are set to automatically lock after 10 minutes of inactivity. This is to ensure that computers are protected if someone forgets to lock their screen, having left it unattended. The Guild will also ensure that staff will shut down their computers at the end of every day.

Passwords

Each member of staff shall have their own unique login and strong password to access the Guild's systems. Logins or passwords shall not be shared. The access/permission levels will be determined by the supplied login credentials.

When creating a strong password, the following should be adhered to:

- The password shall contain at least one upper case character, one lower case character, one number, one special character and shall be at least 12 characters long.
- No previous passwords shall be used.
- The password for each application shall be different unless it uses single sign on.
- The password shall not be easy to guess like job titles, birthdays, names.
- No easy combinations such as 1234 or ABCD shall be used.

- Training will give guidance around the use of sentences or three memorable words.
- The password shall be kept confidential.

Each member of staff shall take the following precautions in relation to passwords:

- Ensure that nobody is looking over their shoulder when they create the password or when they type it into a device.
- Shall not write their password down or email it to anyone, including themselves.
- Shall not say their password out loud or hint at how they created it.
- Shall change their password if they believe someone else knows it.
- Shall notify their manager or DPG immediately if they believe their password has been compromised.

Password management software

- All staff have access to a solution for encrypted password management.
- Accessing passwords is subject to two factor authentication and a master password.
- The Operations Manager and ICT Senior Coordinator have global admin access.

Encryption

The Information Commissioner's Office (ICO) highlights the importance of encryption as a level of protection for electronic personal data. will, therefore, ensure that:

- All laptops are encrypted using BitLocker automatically
- All removable media, including memory sticks, are encrypted using BitLocker
- Our Operations Team is the only Team that rely on VPN access. That VPN will be encrypted.

Access Control

The Guild will ensure that suitable permissions and access controls are in place in respect of electronic personal data. This will ensure that access to personal data will only be given to those that need it to conduct their roles.

Anti-Malware

The Guild realises that its systems are constantly at risk of being attacked by malicious malware that could penetrate its systems and access the personal data it is responsible for and/or corrupt it. Therefore, it will install and keep up to date suitable anti-malware which will protect its systems against:

- Viruses,
- spyware,

- worms,
- trojans,
- ransomware, and
- anything designed to perform malicious operations on a computer.

Back-Ups

The Students' Guild acknowledges the importance of regularly backing up its systems so that it always has a copy of its electronic information. We will make every effort to ensure that it regularly backs up its systems at least once a day and keep the backup where possible in a secure location within the UK or EU.

Cloud Computing

The Students' Guild will ensure that:

- It carries out a Data Protection Impact Assessment (DPIA) before adding more or changing cloud providers.
- It has suitable Data Processing Agreements with existing and new cloud providers.
- It adheres to the ICO Code of Practice on cloud computing.
- It takes appropriate technical and organisational measures to safeguard the data processed in the cloud.
- The data is processed within the EU, if possible but if this is not possible, the Students' Guild will:
  i. Only allow the processing of personal data to take place in countries that have an adequate level (UK and EU GDPR grade) protection for personal data (i.e.: an adequacy decision).
  ii. Enter into UK and EU GDPR compliant contracts with the cloud providers.
  iii. Ensure that appropriate safeguards are put in place in accordance with Article 46 of the UK GDPR and, where relevant, the EU GDPR.

AI Security Measures

The Students' Guild will ensure that:

- We regularly review the AI tools we use to ensure they remain compliant and secure.
- Staff are trained in getting the most out of AI and understand the risks associated with sharing personal data or company sensitive data with generative AI chat.
  - Do not install AI software from external sources without it going through a Data Privacy Impact Assessment

CONFIDENTIALITY

The Students' Guild shall ensure that all employees who have access to and/or process personal data are contractually bound to keep it confidential.

SECURE DESTRUCTION AND DELETION

Personal data, which is no longer required, should be disposed of in accordance with this policy and the Student Guild's Retention Policy. By following the procedures below, the Guild aims to minimise the risk of any unauthorised or unlawful access to or use of personal data.

Hard Copy Personal Data

When paper files containing personal data are no longer required, they will be destroyed in such a way that they cannot be reconstituted. All personal data will be treated as confidential data and the documents will be posted into locked confidential waste bins. Items marked for disposal are not to be stored insecurely, such as on desks, on top of cupboards or on bookshelves but rather posted into the confidential waste bin immediately.
The Guild makes use of confidential waste bins which are managed by an external company. The Guild does not have access to the keys for these bins, and they are emptied regularly,

If a large number of documents are to be disposed of, they will be placed in confidential waste 'Shred-it' sacks and sealed. The sacks must be stored in a secure location until they are collected by the university porters and taken away by the university's approved waste disposal contractor.

Electronic Personal Data

Electronic personal data, which is no longer required, should be securely deleted in accordance with this policy and the Guild's Retention Policy. By following the procedures below, the Guild aims to minimise the risk of any unauthorised or unlawful access to or use of electronic personal data.

Secure deletion has not been defined but the ICO consider that a plain English interpretation implies 'destruction'. This means that the electronic personal data must be irretrievably destroyed, such that it cannot be recovered. It does not mean that it has simply been deactivated or archived, such that it could be re-instated. If electronic personal data has been archived, it will be treated as 'live' and the UK GDPR will apply.

Emails

When emails containing personal data are no longer required, they should be electronically deleted and then deleted from the deleted box. They should not be archived, unless there is a need to keep them, as the archives are simply another folder in which to store live data.

Other Electronic Personal Data

When files containing electronic personal data need to be deleted, they should be electronically deleted and then deleted from the recycle bin.

Electronic Equipment

Electronic equipment includes items such as printers, photocopiers, scanners, laptops, computers, tablets, digital media such as CDs, DVDs, USBs, and any other device which processes personal data.

All electronic equipment which processes personal data must be securely destroyed using a reputable company and a Certificate of Secure Destruction must be obtained as evidence. This Certificate must be retained and produced to the ICO, if necessary.

The contract with the company that will securely destroy the electronic equipment should contain suitable clauses to confirm that they will comply with the data protection legislation and take appropriate technical and organisational measures to safeguard the personal data until it is securely destroyed. If the contract does not contain suitable data protection clauses a UK GDPR compliant and suitably drafted data processing agreement should be entered into.

If any electronic equipment is leased, such as a printer or photocopier, appropriate steps must be taken to ensure that any personal data on the hard drive has been irretrievably destroyed before it is returned to the provider.

The contract with the provider of leased items must confirm that they will adhere to the data protection legislation and, in particular, that they will check that all personal data on the machine/device has been irretrievably destroyed before return.

Electronic equipment must also be disposed of in line with the EU Waste Electrical and Electronic Equipment (WEEE) Directive and the UK Electrical and Electronic Equipment Regulations.

DATA PROCESSING AGREEMENTS

The UK GDPR requires that if Controllers instruct Processors to process personal data, they must enter into data processing agreements with them, and those contracts need to set out all the requirements specified within Article 28 of the UK GDPR. Therefore, if the Students' Guild instructs third party processors to carry out work for them such as external payroll, IT, and cloud services providers**,** the Guild will need to enter into a data processing agreement with them to ensure that they adhere to all the requirements under the UK GDPR and in particular, security.

BREACHES

Any breach of this policy should be reported to Data Protection Guardian immediately, who will implement the data breach process if necessary.

POLICY REVIEW

This policy will be reviewed every two years or when a significant change to the policy occurs. This is tracked via the Guild's Policy review Framework. All Policies will be approved by Trustees and the Senior Leadership Team.

Document History

Date	Version	Created by
Pre 2015	1.0	Edmund Philips
25/05/2018	2.0	Mark Johnson
16/09/2023	2.1	Mark Johnson
13/10/2025	3.0	Mark Johnson