DATA PROTECTION 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**" or "**Guild**" which is a registered company 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.

The University of Exeter Students' Guild is committed to the protection of the personal data of people with whom it deals with. This includes current, past, and prospective employees, students of the university of Exeter who are automatically members of the Guild and others with whom it communicates. This personal data must be dealt with properly, however it is collected, recorded, and used

PURPOSE OF THIS POLICY

The purpose of this policy is to set out how the Guild handles personal data. This policy should be read at induction and updates circulated as and when necessary.

This document sets out the obligations regarding data protection and the rights of people with whom it works with in respect of their personal data under the UK General Data Protection Regulations (UK GDPR), Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and other applicable laws. It also applies to non-UK laws such as the EU General Data Protection Regulation which might apply in certain circumstances. These and all other applicable laws are collectively referred to as 'Applicable Laws' in this policy.

SCOPE OF THIS POLICY

The Students' Guild is a data controller under the UK GDPR. It may also be a data processor in some situations.

This policy applies to all the Guilds' personal data processing functions, including those performed on students, employees, contractors, the University of Exeter, and any other personal data the organisation processes from any source.

- This policy covers all aspects of handling information, including (but not limited to):
- Structured record systems – paper and electronic.
- Transmission of information – email, cloud sharing, post, and telephone.
- Information systems managed and/or developed by or used by the Guild. e.g., our student membership systems.

RESPONSIBILITIES

Students' Guild Career Staff

The Guild holds various items of personal data about its employees which are detailed in the relevant privacy notice at https://www.exeterguild.com/privacy. Employees must ensure that all personal data provided to the Guild in the process of employment is accurate and up to date.

During day to day working, it is likely that staff will process personal data. Prior to handling any data, staff are required to have completed the data protection training course which includes UK GDPR and Cyber Security. In addition to this, staff must maintain a current knowledge of data processing best practice through training updates, delivered by the Operations Manager. When handling personal data, staff are required to follow the guidance set out in the data protection and information security policies.

Students' / Casual staff

Society committee members, representatives, volunteers and student staff may handle personal data to administer their activities and services. Students handling such data are required to have completed the Guilds' Data Protection training prior to receiving permission to handle any personal data related to Students' Guild activities and services. When handling personal data, students are required to follow the guidance set out in the data protection and information security policies,

including the reporting of data breaches, respecting the rights of individuals and secure processing procedures. Details of the training can be found at www.exeterguild.com/privacy.

Students' Guild Managers

Guild managers must ensure that staff handling data during 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 policies. Managers are also required to conduct termly audits of their relevant spaces and processing activity to identify weaknesses in information security

Data Privacy Guardian

This role of Data Privacy Guardian (DPG) is held by the Guilds Operations manager and will oversee the day-to-day data protection activity. All matters regarding personal data that requires escalation will be dealt with internally by the Data Privacy Guardian in the first instance.

Other responsibilities are:

- Being first point of contact for reporting data breaches or any other data incidents
- Receiving and processing data subject access requests
- Liaising with the appointed DPO for support and guidance to ensure compliance
- Report to Finance & Risk Committee the organisations Operational Compliance Dashboard
- Ensure the organisation is sufficiently trained in Data Protection
- Report all Data Protection activity and risk to SLT and trustee subcommittee level
- Liaise with the University's information governance team for alignment
- Ensure we have a sufficient SLA with an external consultant that can deliver the DPO roll

Data Privacy Guardian's contact details

Operations Manager
University of Exeter Students' Guild
Devonshire House
Stocker Road
Exeter
EX4 4PZ
data-protection@exeterguild.com

Data Protection Officer

The Data Protection Officer (DPO) role is provided by an external consultancy. The DPO is delegated authority by the Chief Executive to carry out the role with the resources required to be effective in the protection and security of the personal data the organisation handles.

The role of DPO is responsible for:

- Informing and advising the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws
- Monitoring compliance with the UK 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
- The DPO will oversee the DPG when handling data subject requests to ensure compliance at all times.

Data Protection Officer's contact details

Data Protection Officer
Data Privacy Advisory Service
Unit 14,
Dunchideock Barton,
Dunchideock,
Exeter,
Devon.
EX2 9UA
dpo@dataprivacyadvisory.com

UK AND EU GDPR CONTEXT AND DEFINITIONS

The UK General Data Protection Regulation (UK GDPR) is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR). The UK GDPR is the UK's privacy law that governs the processing of personal data within the UK.

TRAINING

All Guild staff, whether they are student or career staff, are required to complete Data Protection training. Our data protection training covers all aspects of Data Protection and Cyber Security from UK GDPR, the Data Protection Act 2018 and Cyber Security good practice including how to spot, deal with and report cyber threats of varying types. Staff must complete this training before commencing in their role at the Guild. The Guild also run frequent Cyber Attack Simulations to test the organisations posture when facing threats of that nature.

COMPLIANCE

Respecting Individuals Rights

The General Data Protection Regulations sets out a series of rights for individuals. Guild employees planning data processing activities must record how these rights are addressed. The data protection and information security handbook detail the rights and the organisation's standardised processes to meet these individual rights.

Processing Special Categories of Data

The Students' Guild processes special categories of data. The Guild ensured this data is collected lawfully. This data may be analysed in broad terms where no direct link to an individual can be made.

Subject Access Requests

The Subject Access Request policy details the procedures on how subject access requests must be handled. Any individual or department receiving a Subject Access Request must share this with the Data Protection Guardian immediately. The DPG shall respond to the request promptly and aim to fulfil the request without delay and at the latest within one calendar month of receipt.

Lawful Data Processing

The Students' Guild shall only process data within the law. Where a lawful process has been identified; the Data Protection Guardian must make a record of the lawful justification within the privacy notice.

Children
The Guild ensures it applies stronger safeguards to data belonging to those under the age of 18. This includes:

- Only collecting data necessary and minimising its retention period.
- Conducting DPIAs where necessary
- Ensuring additional technical measures are in place to ensure the tighter security of this data.
- Limiting any marketing

Any student volunteer working with children will be subject to undertaking and passing a DBS check.

DBS Checks
The Students' Guild handles personal data when facilitating the Disclosure and Barring Service applications process. This is done securely and in line with the DBS's code of practice. The Students' Guild will keep a record of applications, name and application reference number, for compliance purposes and only retain in accordance with the Guilds' data retention policy.

Data Breaches
The Students' Guild shall adopt processes to detect data breaches including audits and other appropriate processes. Career and student staff shall report data breaches as outlined in Data Protection Training and via the Operations page of the Guild Hub

Where an employee, casual staff member, supplier or contractor discovers a data breach, they must report this to the Data Protection Guardian within 24 hours. The Information Commissioner's Office shall be notified within 72 hours of the breach where it is likely there is a risk to the rights and freedoms of individuals. 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 training and in the Operations page of the Guild Hub

Data Protection by Design
Employees are required to adopt a privacy by design approach to everyday activities. However, when planning projects that involve the collection and processing of personal data, a Data Privacy Impact Assessments (DPIAs) must be completed. This will be reviewed by the DPG in the first instance and escalated to the DPO if necessary. Details of how to conduct DPIA's are within the Operations page of the Guild Hub.

USING AI

Artificial Intelligence (AI), especially Generative AI, is becoming a valuable tool in how we work, communicate, and create. As part of our commitment to transparency and responsible data use, this section explains how we use AI in ways that protect personal information and respect individual rights.
Whether it's helping summarise information or generate content, we ensure that any data used with AI tools is handled carefully, with privacy and fairness in mind. We avoid using sensitive or special category data (e.g., health, ethnicity, political views), only use tools that have undergone a Data Privacy Impact Assessment (DPIA), and always include human oversight in decisions that affect people. This helps us stay open, inclusive, and aligned with our values while keeping data safe.
We do not use AI to make fully automated decisions that have legal or significant effects on individuals without meaningful human involvement.

Responsible Use of AI

- Guild staff are encouraged to explore and use AI tools to enhance their work. When doing so, they will avoid including personal or sensitive company data. This helps maintain strong data security and ensures compliance with our policies.
- Special category data relating to individuals will not be inputted into Generative AI tools. Identifiers should be removed before use.
- Guidance around responsible AI use will be provided as part of Cyber Security training.
- Generative AI tools will have undergone a DPIA before business use.
- If AI tools are used to process personal data (e.g., summarising interviews or analysing feedback), informed consent must be obtained.
- Where third-party data is involved, ownership and usage rights must be clarified and documented in the DPIA.
- We regularly review the AI tools we use to ensure they remain compliant, secure, and aligned with our values.

Types of AI Tools in the Workplace

1. **Integrated AI Assistants (e.g., Microsoft Copilot)**
    - Embedded in tools like Word, Excel, Outlook, and Teams
    - Designed for productivity, summarising content, drafting emails, analysing data
    - Comes with enterprise-grade privacy and security controls
2. **Other Generative AI Chatbots (e.g., ChatGPT, Gemini)**
    - Used for brainstorming, drafting, summarising, and answering questions
    - May be web-based and vary in terms of data privacy and retention
    - Requires careful consideration before inputting data to ensure it is not sensitive
3. **AI-Powered Search and Knowledge Tools**
    - Combine search engine capabilities with generative responses
    - Useful for research, quick answers, and summarising web content
    - Often connected to the internet, so data input should be non-sensitive
4. **Specialised AI Tools**
    - Focused on specific tasks like writing enhancement, transcription, video creation, or image manipulation
    - The Guild may use other AI models behind the scenes but would be task-specific

SECURITY

All employees are responsible for ensuring that any personal data that the Guild holds, is kept securely and is not disclosed to third party unless that third party has been specifically authorised by the Guild to receive that information and has entered into a confidentiality agreement by way of a contractual Data Processing Agreement.

All personal data should be treated with the highest security and must be kept in accordance with all policies relating to the security of personal data

Final approval of any policies relating to the security of personal data is made by the Finance & Risk Committee.

Communication of this policy to those affected is the responsibility of DPO.

Compliance and oversight is managed by the DPG, in consultation with the Finance & Risk committee and the DPO.

Data must be secured:

- In a lockable room with controlled access.
- In a locked drawer or filing cabinet.
- If computerised, password protected or protected with access control in line with the cyber security policy.
- Stored on (removable) computer media which are encrypted in line with the Cyber Security Policy.

All staff are required have undertaken an in-person ICT induction and signed the corresponding documentation. This induction covers aspects of the Computer Misuse Act 1990, acceptable use of hardware and guidance around what to do when faced with cyber security and data protection incidents / breaches. This must have been completed before they are given access to organisational information of any sort.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation.

Personal data may only be deleted or disposed of in line with secure destruction and deletion policies and procedures. For example, manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately and securely destroyed before disposal.

RETENTION AND DISPOSAL OF DATA

The Guild shall keep personal data in a form that permits identification of data subjects for no longer than is necessary, for the purpose(s) for which the data are processed.

The Guild may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Retention Schedule within the Data Retention Policy along with the criteria used to determine this period including any statutory obligations the Guild has to retain the data.

DISCLOSURE OF DATA

All personal data should be accessible only to those who need to use it.

The Students' Guild must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Guild business.

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
12/05/2021	2.1		Mark Johnson
22/10/2025	3.0		Mark Johnson