



## Data Protection Policy

<b>Policy Name:</b>	<b>Data Protection Policy</b>		
<b>Approval Date:</b>	12/02/2025	<b>Review Date:</b>	February 2026

### REVIEW HISTORY

Date	Name	Signature	Notes
------	------	-----------	-------

## 1. Introduction

- a. The Union understands and places great importance on the General Data Protection Regulation. This policy refers to both electronic and physical data the Union controls and processes.
- b. In this policy, "website" refers to [www.goldsmithssu.org](http://www.goldsmithssu.org)
- c. GSU takes the security of personal information very seriously. We make sure that personal data is only accessed for legitimate purposes by individuals who are authorised to do so.
- e. All of the Leadership Team are responsible for ensuring this policy is implemented within their areas of operation and supporting the Data Protection Officer in conducting their duties.
- f. All employees/volunteers must follow this policy without expectation, and a failure to do so could result in disciplinary action.

## 2. Background

The Students' Union needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include students, employees (present, past and prospective), suppliers and other business contacts. This information includes name, address, email address, dates of birth, private and confidential information and occasionally sensitive information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hard copy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with the UK



General Data Protection Regulations (GDPR). Use of data is compliant with the Data Protection Act 1998 and General Data Protection Regulation.

### **3. How We Use Your Information**

Goldsmiths SU processes data for a range of reasons including

- Administration of Membership Records (including processing for not for profit organisations)
- Fundraising
- Advertising, Marketing and Public Relations
- Accounts and records
- Consultancy and Advisory Services
- Employment Administration
- Crime Prevention and Prosecution of Offenders
- Research
- Use of data is compliant with the Data Protection Act 1998 and General Data Protection Regulation.

### **4. How You can Edit Your Personal Profile**

We realise that your Personal Information, including your name, address and email address, is subject to change. To the extent that you do provide us with Personal Information, we wish to maintain its accuracy.

In some cases, we provide a means to create an account or a profile of information. For example, to change your Personal Information, log in on our website as usual and select the profile icon at the top right hand side of each page.

### **5. Data Sharing with Goldsmiths College**

We have a data sharing agreement with Goldsmiths College.

This agreement permits the transfer of all or part of your personal information from Goldsmiths College to Goldsmiths SU for a range of purposes in relation to the legitimate pursuit of our activities. These include provision of support services, such as viewing your student records with your permission, or Goldsmiths sharing your data with us when we are representing you, participation in democratic processes, communications relating to your membership and involvement in quality assurance systems such as the department representative programme.

You can tell Goldsmiths College that you do not wish Goldsmiths SU to receive your data by opting out at enrolment or by withdrawing your permission by logging on to My Goldsmiths. You can also opt-out of communications via links within emails. However, involvement in our activities where you give us your information directly is not covered by this specific data sharing arrangement.



We will disclose information relating to extra-curricular activity to Goldsmiths College for a number of reasons. This will include administration of your Higher Education Achievement Record (HEAR) or a complaint and appeal concerning your status as a student.

In these cases, you will be asked to give us specific consent to give this information to Goldsmiths College. If you do not consent – this information will not be included on your HEAR or we will offer limited guidance in relation to your complaint and appeal.

## **6. Disclosure of Information To Others**

Your information will not be sold, traded, or rented to individuals or other entities. However, we may need to share your information with third parties to charge your credit card or deliver specific services to you such as support services. These third parties are required not to use your information other than to provide the services requested by Goldsmiths SU.

We may disclose your information if we believe in good faith that such disclosure is necessary to:

- a. comply with any relevant legal obligations or
- b. protect and defend the rights or property of Goldsmiths SU

We will share information with Goldsmiths College or the emergency services without your permission only in cases where there is a belief you are at risk of immediate harm to yourself or others, or where it is required by law, for crime prevention, investigation or detection purposes. This decision will be made by the Chief Executive or their nominated deputy.

## **7. Security of Your Personal Information**

We safeguard the Personal Information you send to us with certain physical, electronic, and managerial procedures.

We also store your Personal Information behind our firewall and utilise appropriate security measures in our physical facilities to prevent loss or unauthorised use of sensitive information. Except as provided elsewhere in this Privacy Policy, we limit access to Personal Information in electronic databases to those persons, including Goldsmiths SU employees and full time student officers, in our organisation that have a need for such access.

While we strive to protect your Personal Information, we cannot ensure the security of the information you send to us, and so we urge you to take every precaution to protect your Personal Information when you are on the internet.

We suggest that you change your passwords often, use passwords that include a



combination of letters and numbers, and use a secure browser. Products and services are available which can help give you privacy protection while navigating the internet. While we do not anticipate breaches in security, if one occurs, we will use all reasonable efforts to correct the problems that led to the breach.

## **8. Job applicants, current and former Goldsmiths SU employees**

When individuals apply to work at Goldsmiths SU, we will only use the information they supply to us to process their application and to monitor recruitment statistics.

Where we want to disclose information to a third party, for example where we want to take up a reference or obtain a 'disclosure' from the Criminal Records Bureau we will not do so without informing them beforehand unless the disclosure is required by law.

Personal information about unsuccessful candidates will be held as detailed below, it will then be destroyed or deleted. We retain de-personalised statistical information about applicants to help inform our recruitment activities, but no individuals are identifiable from that data.

Once a person has taken up employment with Goldsmiths SU, we will compile a file relating to their employment. The information contained in this will be kept secure and will only be used for purposes directly relevant to that person's employment. Once their employment with Goldsmiths SU has ended, we will retain the file as detailed below.

## **9. Children and Under 13s**

We need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.

For children under this age we need to get consent from whoever holds responsibility for the child and seek to explain to these individuals and the child themselves what data we're holding and why.

## **10. Summary of where data is currently held**

This table seeks to clarify where data is being processed within the organisation, and will be updated on a regular basis. It was last updated in February 2024.



Type of Data	Data Processor	Type of Data Held by Goldsmiths SU	Who has Access	Legal Based Used	Length Data Stored
Members/ Public/Em ployees	Gmail	Personal and Sensitive Data	Relevant GSU staff members	Consent	Kept on file unless asked by member to delete.
Members	Google Forms	Personal and Sensitive Data	Professional GSU Staff Members	Consent	End of survey/ Academic year in compliance with GDPR
Members	Mailchimp Database	Personal name, Student email, Age data	Communications Team	Consent (option given to unsubscribe)	End of subsequent third academic year after data collected
Members/ Public	MSL Database	Personal and Sensitive Data	Communications Team, Chief Exec, select staff within the Membership team	Legal / Contract via College / Consent via College	End of the subsequent third academic year
Elected Officers	Front of Website	Names of elected officers and staff, candidates, contact	Public	Consent/ Contract	When new officers take role



		details, photos			
Members/ Customers/ Public	Google Analytics	IP Addresses	Communications Team	Consent	IPs not accessible in reporting modules
Members/ Public	Facebook	Determined by individuals. Goldsmiths SU is not data controller	Chief Executive, Communications Team.	Consent	See META Privacy Notice
Members/ Public	Twitter	Determined by individuals. Goldsmiths SU is not data controller	Chief Executive, Communications Team	Consent	See Twitter Privacy Notice
Members/ Public	Instagram	Determined by individuals. Goldsmiths SU is not data controller	Chief Executive, Communications Team, selected officers have limited access	Consent	See META Privacy Notice
Members/ Public	Tiktok	Determined by individuals. Goldsmiths SU is not data controller	Chief Executive, Communications Team	Consent	See Tiktok Privacy Notice
Members/ Public	Photograph y Google Share Drive	Photography at events and photo archive	Professional GSU staff members	Consent	Kept on file unless asked by member to delete.
Employees	People HR	Employee Personal & Sensitive Data	HR - Wala and Nyerho	Legal Obligation	End of subsequent sixth academic year



Applicants	People HR	Applicant CV including name, date of birth and sensitive data	HR - Wala and Nyerho	Legal Obligation	End of subsequent academic year
Members/ Public	CCTV	Time specifics and personal image.	Chief Executive, Commercial Operations Manager, Security Team Leader	Legal Obligation	Twelve months from recording
Members	Advice Pro	Personal & Sensitive Data	Advice Team + HoM	Consent	End of subsequent sixth academic year
Employees	College Share Drive and IT	Payroll details including name, address, date of birth	Chief Executive, Finance Team, HR	Legal Obligation	End of subsequent sixth academic year following end of employment
Customers	Shared Drive	Nursery files including child name, parents name	Nursery Management, Finance Team	Legal Obligation	End of subsequent sixth academic year following end of custom
Employees	Royal London Website	Pension contributions, contact details including name, email address and postal address	Chief Executive	Legal Obligation	End of subsequent sixth academic year following end of employment
Employees	Cowgills	Payroll information including name, date of	Chief Executive, Payroll Provider	Legal Obligation	End of subsequent sixth academic year following



		birth, national insurance number, address			end of employment
Employees	Rotacloud	Name, Email, Hours Worked	Head of Commercial Ops Commercial Ops Manager E&B Manager Retail Manager Head Venue Technician HR Manager Finance Manage	Legal Obligation	End of subsequent sixth academic year following end of employment
Members/ Public	DocuSign	Name Address Phone number Email Address	Head of Commercial Ops Events & Bookings Manager	Issuing Contracts/agreements	We keep for repeat business unless asked to delete.
Employees /Customers	Sage 50	Personal details including name, bank account, gender and date of birth	Finance Team	Legal Obligation	End of subsequent sixth academic year following end of employment or custom





## **11. Responsibilities**

### **11.1 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. Goldsmiths SU 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.

### **11.2 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.

Goldsmiths SU has the right to enact restrictions 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 other rules. When handling personal data students are required to follow the guidance provided at training, respecting the rights of individuals and secure processing procedures.

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.

### **11.3 Union employees (Student Staff)**

The Union holds various items of personal data about its employees. 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.

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.

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.

#### **11.4 Union employees (Non-Student Staff)**

The Union holds various items of personal data about its employees. 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.

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 should 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](http://www.ico.org.uk). When handling personal data, staff are required to follow the guidance.

#### **11.5 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.

All managers will be provided with training by our nominated supplier which they must undertake.

Managers are also required to conduct regular audits of their relevant spaces and IT infrastructure to identify weaknesses in information security. The maximum time frame 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.

If required, the further assessment can help manage data and information:

[Privacy Impact Assessment Template](#)

#### **11.6 Data Protection Officer**

The Data Protection Officer is 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 contact details at the end of this document and their work email address in further instances.

### **11.7 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.

### **11.8 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.

### **11.9 Reporting data breaches**

The General Data Protection Regulation (GDPR) defines a data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

The General Data Protection Regulations further define data breaches into three definition classifications:

- i. "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- ii. "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- iii. "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

During working hours, 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.

## **12. Access to your own personal information**

Goldsmiths SU tries to be as open as it can be in terms of giving people access to their personal information. Individuals can find out if we hold any personal information by making a 'subject access request' under the Data Protection Act 1998. Except for in cases of exemption, if we do hold information about you we will:

- give you a description of it;
- tell you why we are holding it;
- tell you who it could be disclosed to; and
- let you have a copy of the information in an intelligible form.

To make a request to Goldsmiths SU for any personal information we may hold you need to put the request in writing addressing it to the address provided below.

If you agree, we will try to deal with your request informally, for example by providing you with the specific information you need over the telephone, subject to verification of identity.

## **13. About this Document & Contact Details**

This policy was drafted with clarity in mind. However, it does not provide exhaustive detail of all aspects of Goldsmiths SU's collection and use of data. We are happy to provide any additional information or explanation needed. Any requests for this should be sent to the address below:

Chief Executive

Goldsmiths Students' Union

Dixon Road

London

SE14 6NW

Email: [welcome@goldsmithssu.org](mailto:welcome@goldsmithssu.org)

## **14. Further Reading**

Other relevant policies include GSU Social Media Policy. Goldsmiths College's approach to data and privacy is detailed [here](#). For further guidance on matters



relating to Data Protection and Privacy, please refer to the Information Commissioner's Office: [www.ico.gov.uk](http://www.ico.gov.uk).