Data Protection Policy

1. Introduction and general principles

Greenwich Students' Union (GSU or SU) is committed to good practice in the handling of personal data and careful compliance with the requirements of the Data Protection Act 2018.

GSU is committed to good data management, in order to protect people from harm. This means:

- Keeping information securely in the right hands, and
- Holding good quality information.

GSU also ensures that it takes account of the legitimate concerns of individuals about the ways in which their data may be used. In particular, the GSU aims to be open and transparent in the way it uses personal data and, where relevant, to give individuals a choice over what data is held and how it is used.

The most important risks which this policy addresses are:

- Inappropriate disclosure of personal data about employees, individual students, registered guests, members or donors that puts an individual at personal risk or contravenes a duty of confidentiality.
- Negligent loss of data that would cause concern to people whose data was lost and would seriously affect GSU's reputation.
- Failure to engage Data Processors on legally compliant terms. (Data Processors are external contractors and suppliers of outsourced services)

Operational procedures and guidance to paid staff sets out more detailed ways in which these risks can be managed and the objectives achieved.

2 Responsibilities

The Board of Trustees of the GSU recognises its overall legal responsibility for data protection compliance.

Overall responsibility for data protection falls onto the Chief Executive and day to day responsibilities to their nominated Data Protection Officer. The main responsibilities of the Data Protection Officer are:

- Briefing the Board on their and GSU's data protection responsibilities
- Reviewing data protection and related policies
- Advising other staff on data protection issues and practices in SU
- Ensuring that data protection induction and regular training takes place
- Approving unusual or controversial disclosures of personal data
- Approving contracts with data processors (external contractors and suppliers of outsourced services)
- Notification (i.e. registration with the Information Commissioner)
- Handling requests from individuals for their personal data

All staff (and volunteers) are responsible for understanding and complying with the procedures that GSU has adopted in order to ensure Data Protection compliance.

All managers of teams and functional areas have the following responsibilities:

- Assisting the Data Protection Officer in identifying aspects of their area of work which have data protection implications so that guidance can be provided as necessary.
- Ensuring that their activities take full account of data protection requirements.
- Including data protection and confidentiality in the induction and training of all staff and volunteers. (And consultants if relevant)

2.1 Data management

All data collection and recording systems are designed to ensure that the data collected is adequate, relevant and not excessive for the purpose. All staff and volunteers, where relevant, are given training in good data recording practice to ensure that the data they record is appropriate.

GSU takes reasonable steps ensure that information is kept accurate and up to date by asking data subjects at appropriate intervals to check their key information for accuracy and to notify GSU if there have been any changes.

GSU maintains an agreed retention schedule based on legal and practical requirements. This can be viewed at greenwich.co.uk/privacy.

2.2 Retention of Records

The Data Protection Act states that data should not be kept for longer than is necessary for the purposes for which it is processed. Therefore, the SU will use following time periods for retaining employee data. These guidelines relate to all employees at SU who may hold information aboutindividuals.

Employee Data

All application documentation:	1 week
Documentation post interview for jobs who are not successful:	6 month
Ex-employees one to one, appraisal and performance management documents:	6 months
Ex-employees medical history:	1 years
Ex-employees complaints, investigations and grievances:	2 years
Summary of record of service of ex-employees:	2 years
Ex Sabbatical Officer personal details	7 years

It is important to remember that computer records as well as manual files are included in this protocol.

Member data

Once an individual has ceased to be a member of Students' Union, University of Greenwich, any data pertaining them must be kept securely for 6 years. If this is hard copy is must be archived in a secure location or, if the information is on computer it must be filed onto a disc and held securely.

2.3 Disposal of Data

All data on individuals and/or information of any kind must be disposed of sensitively and completely. If the information is hard copy it must be shredded or incinerated. If the information is soft copy (i.e. on a hard drive or computer disk) it must be deleted from the file, disk and the recycle bin of the computer.

3 Confidentiality & security

GSU recognises that a clear policy on confidentiality of personal data – in particular that of donors/members – underpins security. It maintains a policy that sets out which staff and volunteers are authorised to access which data and for which purposes. In particular this clarifies when data may be disclosed outside SU and whether such disclosures require the individual's consent.

GSU maintains a security policy that sets out measures to protect data 'at rest' – including access being restricted only to authorised staff – and measures to protect data 'in transit', whether it is physically removed from a secure environment or transmitted electronically.

All staff, consultants, volunteers and Trustees are required to abide by any security measures designed to protect personal data from loss, misuse or inappropriate disclosure.

4 Use of personal devices and email addresses

4.1 All GSU career employees will be given a University of Greenwich issued laptop for work purposes. Some employees may be issued with a work mobile also if appropriate for their role. Employees should limit their use for personal purposes, ensuring secure use.

4.2 All GSU career employees and some student staff (where appropriate) will be issued with an Affiliate account through the University of Greenwich (University) system. This will allow the employee to access Microsoft 365, Teams for instant messaging, Outlook for emails, the University Portal, Evotix, and other appropriate University systems assigned to Affiliate accounts.

4.3 Career employees should not be using their own laptop, tablet or computer for work purposes. The use of a personal mobile telephone may be required for the submission of expenses through the Basecone application, and/or authentication to get into Office365 or other system through an authentication app. Otherwise, career employees shouldn't be using a personal mobile for work purposes.

4.4 If there is a reason you would like to use a personal device for work purposes (e.g. accessibility needs), please contact GSU HR to discuss.

4.5 If anything happens to a personal device in relation to work purposes (e.g. damage, theft), GSU is not liable to cover any costs of repair or recovery - personal devices not insured by the company.

4.6 If there is a GDPR issue related to the use of a personal device for work purposes, the owner of that device - rather than GSU - may be personally liable.

4.7 Where possible, student staff should have access to a University issued device for any work required during their employment. If this is not possible, then they are to adhere to the University policies on Remote Working and use of own devices.

4.8 Managers of student staff should be mindful not to issue sensitive and/or confidential work or data to student staff who are using their own devices.

4.9 All employees should only be using a University issued email account (e.g. user@greenwich.ac.uk) for work purposes. Personal email addresses (e.g. user@example.com) should not be used to share or receive work related information, especially sensitive and confidential material.

4.10 All employees should use the GSU Data Classification table below to determine how data should be classified, handled and stored in hard copy, digitally, and on devices (work issued and personal).

5 Principles underlying operational procedures

Good data protection practice is, wherever relevant, incorporated into everyday operational procedures. These aim to include:

- Transparency, so that all the individuals about whom data is collected are made aware of the uses that GSU makes of information about them, and in particular to whom it may be disclosed.
- Informed consent, where necessary, especially in the case of donors and clients.
- Good quality data, so that all the data held about individuals is accurate and can be justified as adequate, relevant and not excessive.
- Clear archiving and retention periods.
- Security proportionate to the risk of information being lost or falling into the wrong hands.

6 Specific legal provisions

The General Data Protection Regulation (GDPR) gives rights of access to an individual to the personal data held on them. This is free of charge to request, unless a request is manifestly unfounded, excessive or repetitive. This will be at the discretion of the Data Protection Officer.

- Requests need to be made in writing to the Data Protection Officer. The form for a request is on our website at greenwichsu.co.uk/privacy/. The Data Protection Officer must be satisfied with the identification of the individual making the request and can ask for information or documentation as proof.
- Individuals are entitled to a copy of the information held on them, both on computer and as part of a relevant filing system within 30 calendar days of their request being received.
- Individuals also have a right to know why their information is being held, who that information is being disclosed to and for what purpose.
- An individual must give their consent before any information held about them can be shared with any other agency or body unless the information is required by the police undertaking a criminal investigation.

GSU maintains an up to date Notification with the Information Commissioner as required by law. All contracts between SU and external data processors are reviewed by the Data Protection Officer for compliance with Data Protection Act requirements.

Data Classification table			
Classification Type	**Highly Sensitive**	**Personal/Confidential**	**Non-sensitive/Open**
Description	Inappropriate disclosure of such information may cause **severe damage** or distress to an individual or GSU's objectives and/or reputation.	Inappropriate disclosure of such information may **negatively impact** an individual or the GSU's objectives and/or reputation.	Such information is publicly available to everyone.
Examples	• Highly sensitive information relating to the organisation or other organisations e.g. commercially sensitive information • Sensitive financial information e.g. anything not publicly available. • HR related information, e.g. open case information • Information related to Advice Service cases and/or Check-in Service calls. • Unprotected intellectual property. • Sensitive personal information e.g. race, ethnic origin, politics, religion, trade union, membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation, criminal convictions. Some examples where this might occur include supplementary documents to CVs, equal opportunities forms, sensitive IT information e.g. authentication details.	• Personal information about individuals who can be identified from it. Some examples include salary information, copies of CVs, contact details. • Student information where they can be identified from it. Some examples include Banner IDs, their date of birth (DOB) or contact information. Commercially sensitive information e.g. contractual information, or supplier information provided in confidence.	• Information which is in the public domain e.g. information from our websites or social media, annual financial accounts. • Photographs from GSU events that are posted on our website and/or social media, or used in GSU communications. Information which should be routinely disclosed e.g. some minutes of meetings.

Level of Protection Required	• Such information requires a high level of security control that will ensure its confidentiality and integrity is maintained at all times. It should only be shared under a very strict environment such as: ○ provide only hard copies to authorised individuals in face-to-face meetings and retrieve these copies at the end of a meeting. Where this is not possible, use email, post or hand delivery with the appropriate marking in place. ○ those receiving highly sensitive data must only make additional copies or edits with the originator's authority. • and only on a "need-to-know" basis within GSU or external to GSU, to fulfil statutory and legal requirements. • It should be kept up-to-date and stored in highly restricted areas within centrally managed shared areas or cloud storage, or restricted physical storage areas. Access should be limited to authorised individuals, and appropriate monitoring controls and backup arrangements put in place. GSU and University approved storage facilities should be used where third parties are responsible for data management. • Data should be securely wiped off electronic devices where the device has been decommissioned, or disposal of paper records should follow confidential waste disposal procedures.	• Such information requires the most suitable security controls that will ensure its confidentiality and integrity are always maintained with limited access only on a "need-to-know" basis within GSU or external to GSU to fulfil statutory and legal requirements. • It should be kept up-to-date and stored in highly restricted areas within centrally managed shared areas or cloud storage, or restricted physical storage areas. Access should be limited to authorised individuals, and appropriate monitoring controls and backup arrangements put in place. GSU and University approved storage facilities should be used where third parties are responsible for data management. • Data should be securely wiped off electronic devices where the device has been decommissioned.	• Such information should be available to GSU staff, members and the general public if appropriate permission sought. • It should be stored on centrally managed shared areas or cloud storage areas with appropriate backup arrangements in place. • It should be kept up-to-date and access to it should be limited to only to those authorised to make relevant changes to it. • Disposal should follow normal file deletion or non-confidential paper record disposal procedures.

Information Handling and Device Use Requirements			
Classification Type	**Highly Sensitive**	**Personal/Confidential**	**Non-sensitive/Open**
Paper records			
	GSU areas with restricted access: ✓ Keep files in lockable cabinets/drawers which are locked when not in active use. ✓ No papers left out when away from the desk. **GSU areas with unrestricted access:** × Not permitted **Off-site working** ✓ At home: Should be kept away from public view and stored securely when not in use e.g. kept in lockable cabinets/drawers. ✓ Elsewhere or in transit: Not to be left unattended or in a vehicle (public or private). **Post** ✓ Must be addressed properly to a named individual, sealed and stamped with 'Private and Confidential' with a return address if not delivered. ✓ Use recorded delivery. Hand or courier delivery should also be considered where possible.	**GSU areas with restricted access:** ✓ Keep files in lockable cabinets/drawers when the office is unattended. ✓ No papers left out when away from the desk. **GSU areas with unrestricted access:** × Not permitted **Off-site working** ✓ At home: Should be kept away from public view and stored securely when not in use e.g. kept in lockable cabinets/drawers. ✓ Elsewhere or in transit: Not to be left unattended or in a vehicle (public or private). **Post** ✓ Must be addressed properly to a named individual, sealed and stamped with 'Private and Confidential' with a return address if not delivered. ✓ Use recorded delivery. Hand or courier delivery should also be considered where possible.	✓ Permitted – need to follow good records management procedures.

	✓ It is recommended that the addressed envelope be enclosed in another sealed and properly addressed envelope. Fax: × Not permitted	✓ It is recommended that the addressed envelope be enclosed in another sealed and properly addressed envelope. Fax × Not permitted	
Email			
Between user@greenwich.ac.uk accounts	**REQUIRED** ✓ Only share on a "need-to-know" basis. ✓ If it is ad hoc or one-off document sharing, please password-protect email attachments, sending the password separately to the document in another email or Teams message. ✓ For collaboration work, use Office 365 Teams. ✓ Mark email with private or confidential. ✓ Verify the recipient's address before you click send. ✓ Redact sensitive information from email messages and attachments if not relevant to all recipients particularly from email chains. ✓ Avoid putting Data Subject name(s) in the Subject field, where possible.	**REQUIRED** ✓ Only share on a "need-to-know" basis. ✓ If it is ad hoc or one-off document sharing, password-protect email attachments, sending the password separately to the document in another email or Teams message. ✓ For collaboration work, use Office 365 Teams. ✓ Mark email with private or confidential. ✓ Verify the recipient's address before you click send. ✓ Redact confidential or private information from email messages and attachments if not relevant to all recipients particularly from email chains. ✓ Avoid putting Data Subject name(s) in the Subject field, where possible.	✓ Permitted

	× Not permitted: Auto forwarding to personal email.	× Not permitted: Auto forwarding to personal email.	
From user@greenwich.ac.uk to/from non-university email address: user@example.com	Only where the recipient does not have a Greenwich email account and it is necessary to use this method for a business purpose: **REQUIRED** ✓ Be sure the recipient understands the risk involved, accepts this method, and will treat the data correctly. ✓ Only share on a "need-to-know" basis. ✓ Password-protect attachments with password sent separately (as mentioned above) ✓ Mark email with private or confidential. ✓ Verify the recipient's address before you click send. ✓ Redact sensitive information from email messages and attachments if not relevant to all recipients, particularly from email chains. ✓ Exception to be made for finance purposes related to personal expenses, e.g. claims for GSU staff benefits	Only where the recipient does not have a Greenwich email account and it is necessary to use this method for a business purpose: **REQUIRED** ✓ Be sure the recipient understands the risk involved, accepts this method, and will treat the data correctly. ✓ Only share on a "need-to-know" basis. ✓ Password-protect attachments with password sent separately (as mentioned above) ✓ Mark email with private or confidential. ✓ Verify the recipient's address before you click send. ✓ Redact sensitive information from email messages and attachments if not relevant to all recipients, particularly from email chains. ✓ Exception to be made for finance purposes related to personal expenses, e.g. claims for GSU staff benefits × Not permitted	✓ Permitted

	× Not permitted Sharing any GSU files or communication from user@greenwich.ac.uk to user@example.com	Sharing any GSU files or communication from user@greenwich.ac.uk to user@example.com	
Between two non-university email accounts for work purposes user@example.com to user@example.com	× Not permitted **Only** use your @greenwich.ac.uk account to share.	× Not permitted **Only** use your @greenwich.ac.uk account to share.	× Not permitted **Only** use your @greenwich.ac.uk account to share GSU and/or University information.
Drives			
Shared drives	✓ Where possible, data should be stored in the University's centrally administered Microsoft 365 environment. Where there is a requirement for files to be stored and/or shared confidentially from this environment, set up a folder and restrict viewing/sharing to named individuals, using their @greenwich.ac.uk only. If you need assistance with this, contact the IT Service Desk. ✓ Your individual @greenwich.ac.uk OneDrive can be used for confidential files; please follow sharing protocol above. × Not permitted: using a personal OneDrive or other shared/cloud drive function	✓ Where possible, data should be stored in the University's centrally administered Microsoft 365 environment. Where there is a requirement for files to be stored and/or shared confidentially from this environment, set up a folder and restrict viewing/sharing to named individuals, using their @greenwich.ac.uk only. If you need assistance with this, contact the IT Service Desk. ✓ Your individual @greenwich.ac.uk OneDrive can be used for confidential files; please follow sharing protocol above. × Not permitted: using a personal OneDrive or other shared/cloud drive function	✓ Permitted
C drive – Local machine	× Not permitted	× Not permitted	✓ Permitted/at own risk

drive			of loss as the C drive is not backed up centrally
Cloud storage			
University Centrally Administered M365 including OneDrive for Business, Teams and SharePoint	✓ Permitted Ensure appropriate permissions are assigned to individuals only on a need-to-know basis, whether internal staff or external collaborators. Contact the IT Service Desk for support.	✓ Permitted Ensure appropriate permissions are assigned to individuals only on a need-to-know basis, whether internal staff or external collaborators. Contact the IT Service Desk for support.	✓ Permitted
Non-University Administered Cloud Storage such as iCloud, Google Drive, Dropbox, personally owned OneDrive and any other cloud storage solutions	× Not permitted University data is not permitted for use on non-university administered or non- approved cloud platforms.	× Not permitted University data is not permitted for use on non-university administered or non- approved cloud platforms.	✓ Permitted, as long as account for access is linked to a @greenwich.ac.uk account. However, where possible, data should be stored in the University centrally administered Microsoft 365 environment.
Adobe Creative Cloud	× Not permitted	× Not permitted	✓ Permitted Where possible, data should be stored in the University centrally administered Microsoft 365 environment.

Laptops, mobile and small storage devices			
University-owned laptops	✓ Permitted only where the device is centrally managed by ILS and the user does not have a local super-user account. ✓ Information must be password-protected and only saved temporarily on the C: drive where access to the shared drive is not possible and must be transferred immediately to the shared drive when access becomes available and deleted from the C: drive. ✓ Keep files away from public view when working offsite. ✓ Always use only issued laptops for work purposes and limit its use for personal purposes ensuring secure use.	✓ Permitted only where the device is centrally managed by ILS and the user does not have a local super-user account. ✓ Information must be password-protected and only saved temporarily on the C: drive where access to the shared drive is not possible and must be transferred immediately to the shared drive when access becomes available and deleted from the C: drive. ✓ Keep files away from public view when working offsite. Always use only issued laptops for work purposes and limit its use for personal purposes ensuring secure use.	✓ Permitted
GSU owned mobile phone	✓ Permitted ✓ Ensure device has a password/passcode that is known only to the owner. ✓ Keep files away from public view when working offsite. ✓ Always use only issued phone for work purposes and limit its use for personal purposes ensuring secure use. **Off-site working** ✓ At home: Should be kept away from public view and stored securely when not in use e.g. kept in lockable cabinets/drawers. ✓ Elsewhere or in transit: Not to be left	✓ Permitted ✓ Ensure device has a password/passcode that is known only to the owner. ✓ Keep files away from public view when working offsite. ✓ Always use only issued phone for work purposes and limit its use for personal purposes ensuring secure use. **Off-site working** ✓ At home: Should be kept away from public view and stored securely when not in use e.g. kept in lockable cabinets/drawers. ✓ Elsewhere or in transit: Not to be left	✓ Permitted ✓ Still ensure good security practice, and ensure device has a password/passcode that is known only to the owner. ✓ Always use only issued phone for work purposes and limit its use for personal purposes ensuring secure use. **Off-site working**

	unattended or in a vehicle (public or private).	unattended or in a vehicle (public or private).	✓ In transit: Not to be left unattended or in a vehicle (public or private).
Personal laptops, mobile devices and portable storage devices	× Not permitted In the rare case where an exception is permitted, University security controls are to be enabled on such devices.	× Not permitted In the rare case where an exception is permitted, University security controls are to be enabled on such devices.	✓ Permitted