Data Protection Policy

1 Introduction and general principles

The Students' Union is committed to good practice in the handling of personal data and careful compliance with the requirements of the Data Protection Act 1998.

SU 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.

SU 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 SU 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 SU'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 SU recognises its overall legal responsibility for data protection compliance.

Day to day responsibility for data protection is delegated to the Chief Executive as the nominated Data Protection Officer. The main responsibilities of the Data Protection Officer are:

- Briefing the Board on their and SU'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 SU 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. Where relevant, staff and volunteers are given training in good data recording practice to ensure that the data they record is appropriate.

SU 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 SU if there have been any changes.

SU maintains an agreed retention schedule based on legal and practical requirements. This can be viewed at www.suug.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

Applicants 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

SU 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.

SU 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 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 SU 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.

5 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 www.suug.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.

SU 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.