

Data Protection Policy

Approved by:	Board of Trustees
Date of approval:	10 April 2018
Implementation date:	10 April 2018
Review date (no later than):	31 October 2018
Responsible for implementation:	Chief Executive
Responsible for interpretation:	Board of Trustees

City, University of London Students' Union is a registered charity (charity number 1173858). It is a company limited by guarantee registered in England and Wales (company number 10834450), whose registered office is at Cx118 (Tait Building), Northampton Square, Islington, London, EC1V 0HB.

Data Protection Policy

1.0 Policy Statement

- 1.1 In the course of carrying out its various functions and activities, City, University of London Students' Union (the Union) collects information from individuals and external organisations and generates a wide range of data which is recorded and maintained. The purpose of this policy is to enable the Union to:
- (a) Demonstrate its commitment to the proper handling of personal data;
 - (b) Comply with Data Protection law;
 - (c) Protect the organisation from the consequences of any breach of its statutory and common law responsibilities; and
 - (d) To encourage and support a culture of best practise within data protection.
- 1.2 The Union is a data controller under the provisions of the Data Protection Act (registration number: Z9743163). Personal data is held in compliance with the Data Protection Act (DPA) 1998 and the General Data Protection Regulation (GDPR) post 25 May 2018 and its successors'.
- 1.3 'Personal data' refers to information that identifies a living individual. The Union holds personal data for the following purposes:
- (a) Staff Administration – Appointments or removals, pay, discipline, superannuation, work management or other personnel matters.
 - (b) Advertising, Marketing and Public Relations – Advertising or marketing the business, activity, goods or services and promoting public relations.
 - (c) Accounts and Records – Keeping accounts, deciding to accept a person as a customer or supplier, keeping records of purchases, sales or other transactions, the processing of orders and accounts.
 - (d) Administration of Membership Records, including volunteers and casual workers.
 - (e) Consultancy and Advisory Services – Giving advice or rendering professional services.
 - (f) Benefits, Grants and Loans Administration – The administration of welfare and other benefits.
 - (g) Fundraising – fundraising in support of the objectives of the organisation.
- 1.4 The Union processes personal information about its members in accordance with the principles of the General Data Protection Regulation (GDPR) detailed below:
- (a) Fairly and lawfully and in a transparent manner;
 - (b) Processed for limited purposes;
 - (c) Adequate, relevant and not excessive;
 - (d) Accurate and up to date;
 - (e) Not kept for longer than is necessary;
 - (f) Processed in line with your rights;
 - (g) Secure; and
 - (h) Not transferred to other countries without adequate protection
- 1.5 Complaints can lead to enforcement action being taken so it is vital that the Union has a workable and robust data protection policy that is understood and practiced across all sections of the organisation.

2.0 Background

- 2.1 The Data Protection Act (DPA) 1998 will be replaced by The General Data Protection Regulation (GDPR) post 25 May 2018 define the legal basis for the processing of personal information relating to living individuals’.
- 2.2 The Union is obliged to answer any subject access requests received from individuals. These may be staff, students or any individual who has an association with the Union. They have important rights, including the right to find out what personal information is held on computer and most paper records.
- 2.3 To comply with the first data protection principle of the Act the Union must tell individuals what their personal information will be used for, in particular:
 - (a) Who you are;
 - (b) What you will use their information for;
 - (c) The right to be informed via Privacy Notices;
 - (d) The right to rectification of their data;
 - (e) The right to be erasure (right to be forgotten);
 - (f) The right to data portability;
 - (g) The right to object to restrict/ processing; and
 - (h) Rights in relation to automated decision making and profiling.
- 2.4 Any individual with concerns about how their data may be treated is able to contact and discuss the issue with the Union.

3.0 Management and Staff Responsibilities

- 3.1. The Chief Executive Officer is responsible for the general development, promotion and adherence to this policy, and ultimate responsibility for compliance by all staff.
- 3.2 The General Data Protection Regulation (GDPR) does not specify periods for retention.
- 3.3. All staff who process personal data are expected to understand and adhere to the Data Protection Principles set out in GDPR and to ensure that they dispose of and/or destroy, confidentially where necessary, those records that have reached the end of their retention period.
- 3.4. The Chief Executive is responsible for ensuring that adequate and appropriate knowledge of the GDPR and the Unions legal obligation is available across the organisation. This is achieved by making available this policy and procedures, making training available to relevant groups, making new staff aware through their contracts of employment and working with the Union senior leadership team to raise relevant data protection issues for discussion, resolution and to communicate lessons learnt across the organisation.

4.0 Student Responsibilities

- 4.1 Students should assist the Union in ensuring that their own personal data as provided to the Union is accurate and up to date. Reasonable opportunities to do so will be provided.

- 4.2 Students volunteering for the Union may need to process personal data for activity administration purposes. If students are using personal data they must inform the relevant department manager in charge of the student's activity so that the requirements of the GDPR 2018 can be adhered to.

5.0 Data Collection within the Union

- 5.1 Staff consent to the Union using their data when they commence employment. The data collected includes personal, banking, health, disciplinary and equal opportunities information. You should inform HR of any changes to information that you have previously provided, for example, changes of address or new information relevant to employment.
- 5.2 A confidential reference given to a third party for the purposes of:
- (a) The education, training or employment, or prospective education, training or employment, of the data subject;
 - (b) The appointment, or prospective employment of the data subject to any office; or
 - (c) The provision, or prospective provision, by the data subject of any service.

Will remain confidential, and is exempt from the subject access provisions, in that the subject cannot gain access from the person providing the reference. References should be marked confidential.

References may be accessible to the data subject if received from a third party. Your reference could become accessible from the person to whom it is sent. Care should be taken to ensure that any reference given by you is founded on fact and that viewpoints expressed can be justified.

- 5.3. The Union Academic Advice Service has a Confidentiality Policy and their service users consent to the Union contacting third parties when they sign a form of authority. Personal data will only ever be processed in accordance with these consents.
- 5.4 Other Union departments hold information in relation to its members in order to contact students with information which may be of value to them. This can be related to volunteering placements, employment placements and media contacts. Members have the option to opt out of the Union but by joining give their consent to such information being collected. Information is also collected via our website for those joining student groups.
- 5.5 In most cases the Union will refrain from processing data relating to sensitive personal information as these matters have the potential to be used in a discriminatory way.
- 5.5.1 This includes details relating to an individuals' ethnicity, religion, political opinions, health conditions, sexuality, criminal records etc. Where this is unavoidable, e.g. in the case of health and safety records, access will be limited to specific members of staff only. In circumstances where this information is required for the data processing purpose, access will be limited to specific members of staff only. Data subjects will also be required to give informed consent to the Union to use their sensitive information.

6.0 Data Sharing, Data Security and Disposal

- 6.1 In order to prevent unauthorised processing, or accidental loss, damage or destruction, records that hold personal data are stored in locked filing cabinets, and access to IT drives, applications and servers is managed by password only.
- 6.2 Data is shared across business functions and between staff of the Union only when it is required in order for them to perform their work function. Data is shared with external agencies, such as local authorities, the police upon request, and other organisations for volunteer and work placements. As far as possible data is transmitted solely over the secure network and the transmission of data via paper, post or independent electronic devices is strongly discouraged. The Union network is a secure system with fully managed access control, back-up and recovery processes in place, managed by City, University of London.
- 6.3 Where the information held on a laptop or other portable device could be used to cause an individual damage or distress, in particular where it contains financial or medical information, they will be encrypted. The level of protection provided by the encryption should be reviewed and updated periodically to ensure that it is sufficient if the device was lost or stolen; you may need to seek specialist technical advice. In addition to technical security, organisations must have policies on the appropriate use and security of portable devices and ensure their staff are properly trained in these. If it is brought to the Commissioner's attention that laptops that have been lost or stolen have not been protected with suitable encryption s/he will consider using enforcement powers.
- 6.4 Data is retained and disposed of according to need and in conjunction with the Data Records Retention Schedule. At the end of the retention period data are disposed of and/or destroyed, confidentially where necessary. Manual files are shredded and electronic data is deleted from central systems.
- 6.5 A third party 'Memberships Solutions Limited ('MSL') will provide an information management system to store and manage our students' personal information. MSL are bound by a contract stating that personal information will not be modified, deleted, or shared, without the instructions of the Union, or used for any purpose other than that specified by the Union. They are also contractually obliged to abide by the General Data Protection Regulation. The system provider is subject to change; any future provider will be added to this policy.

7.0 Sharing Data Routinely with Other Organisations

- 7.1 The Union has no responsibility for the management of personal data processed by City, University of London, which is solely responsible for its own compliance with the Act and GDPR. City, University of London provides a separate notification to the Information Commissioner and is responsible for responding to requests for access to information in its possession.
- 7.2 The Union reserves the right to share information with the City, University London as necessary to pursue its legitimate interests, or to ensure the smooth operation of procedures and practices in the interests of students, staff and other individuals connected to the Union. Disclosure of personal data is always made in accordance with the GDPR and never prejudices an individual's rights or freedoms.
- 7.3 Under circumstances relating to disciplinary activity both the Union and the City, University of London reserve the right to pass necessary information to the other in order to uphold and enforce disciplinary procedures.

- 7.4 Disclosure of personal data is always made in accordance with the principles of the General Data Protection Regulation 2018 and never prejudice an individual's rights or freedoms.
- 7.5 In the case of personal information requests by the Police or a similar third party for the purposes of the prevention or detection of crime or for taxation, and where it is not appropriate for the requestor to seek that information from the individual(s) concerned, it may be deemed necessary to release personal data to the third party. The General Data Protection Regulation allows for a data controller (the Union) to release personal data for the purpose of:
- (a) The prevention or detection of crime;
 - (b) The apprehension or prosecution of an offender; or
 - (c) The assessment or collection of any tax or duty or of any imposition of a similar nature.

Unless a Court order is made, the decision regarding whether to release personal data will belong to the Union.

8.0 Request for Information, erasure and modification

- 8.1 In order to fulfil their responsibilities under the act the organisation may, before responding to any request, seek proof of the requestor's identity and any further information required to locate the personal data requested.
- 8.2 On receipt of a request the Union's Senior Leadership Team will automatically be asked to supply copies of any data concerning the individual which they hold.
- 8.3 Individuals have the right to request what personal information is held about them on computer and can get access to most paper records. The General Data Protection Regulation gives you, as a "Data Subject" the right, of access to receive details of all personal information which concerns you and which is stored and processed by the Union. Request for such information should be made by completing the attached form at Appendix 3 and forwarding it to the Chief Executive. It should be accompanied by a copy of your identity document (such as passport, drivers licence or student Identity Card).
- 8.4 The General Data Protection Regulation requires the Union to provide you with your information within 30 days.
- 8.5 On occasion the Union will process personal information to improve offers and services to enhance the student experience. This may involve profiling or automated decision making based on student information (e.g., if they are a member of a XXX club) or information passed from the University (e.g., the department the student belongs to). If you would like to object to your personal information being processed to improve the Union offers and services, you can contact us at: studentsunion@city.ac.uk.

There may be a legal basis to continue processing your data in this way, but you are entitled to an explanation of the processing and the opportunity to challenge them.

- 8.6 If you would like any of your personal information held by the Union to be blocked, erased, or destroyed, you should contact us at: studentsunion@city.ac.uk.

- 8.7 In some cases (e.g., records relating to a criminal investigation) there may be legitimate reasons for the Union to preserve your personal information. Once legitimate purposes are no longer valid, the Union will endeavor to honor your requests.
- 8.8 Please note however, that some personal information held by the Union is obtained from the University and so you would be required to work with the University Registry Department to remove any personal information held on University systems. On such occasions students should contact the University's Student Office (020 7040 8321 registry@city.ac.uk).
- 8.9 As a students' union, the Union is not a "public authority" in the sense of the Freedom of Information (Fol) Act. This means that records of the Union itself will not be covered by Freedom of Information, and cannot be requested under Fol. It is also unlikely that the Union would be considered to be covered by the Environmental Information Regulations (the definition of a "public authority" in the Regulations is broader and vaguer than that in the Freedom of Information Act).
- 8.10 Records which the University holds about the Union, including communications with the Union and information provided to the University by the Union, are covered by the Freedom of Information Act and the Environmental Information Regulations, and can be requested from the University.

9.0 Marketing and Communications

- 9.1 When registering with the University, students can consent for some personal details to be passed to the Union for administrative and communication purposes. Unless students have opted out, occasionally throughout their time at the University, the Union will communicate with students via email. This will be for the main purpose of communicating offers or services provided solely by the Union in line with the students' membership.
- 9.2 If students would like to be removed from a mailing list they may opt out of that type of communication using the unsubscribe link provided in the email. Communications will not contain information that would not be reasonably expected given the relationship between student and the Union.

10.0 Data Breach

- 10.1 According to the General Data Protection Regulation appropriate security of personal data is required, including protection against unlawful processing and against accidental loss or damage. To ensure this, electronic information is stored on internal servers managed and controlled by the Union or securely maintained on external servers by partners bound by data protection contracts. In the unlikely event of a data breach, staff have been trained to inform the Data Protection Officer who will carry out the necessary procedures.

11.0 Complaints

- 11.1 Individuals concerned about any aspect of the management of personal data at the Union are able to raise their concerns in a fair and equal way. Complaints can be registered with the Chief Executive. If an individual is not satisfied that their complaint has been properly dealt with they should contact the Chair of the Union Trustee Board.

- 11.2 If an individual feels they are being denied access to personal information they are entitled to, or feel that their information has not been handled according to the eight principles, they can contact the Information Commissioners Office:

The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Tel: 01625 545700

Website: www.informationcommissioner.gov.uk

Data Retention Schedule

Description of data in Personnel	Retention Period	Reason for Retention Period	Action Following Retention Period
Staff application forms; interview notes (unsuccessful applicants)	12 months from the date of interviews	Limitation period for litigation	Shred hard copy files, delete data files
Personnel files containing training records, absence history, details of contractual changes and reasons for leaving	Minimum 6 years from the end of employment (up to 10 years – space permitting)	Provision of references and limitation period for litigation	Shred hard copy files, delete data files
Facts relating to redundancies	3 years from the date of redundancies	Limitation period for litigation	Shred hard copy files, delete data files
Income Tax and NI returns, correspondence with Tax Office	6 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993	Shred hard copy files, delete data files
Statutory Maternity Pay records and calculations	3 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986	Shred hard copy files, delete data files
Wages and salary records	6 years from the last date of employment	date of employment Taxes Management Act 1970	t Act 1970 Shred hard copy files, delete data files
Medical Records kept by reason of the Control of Substances Hazardous to Health	40 years	COSHH 1994	Shred hard copy files, delete data files
Membership information, including society/sports/volunteers/media	Up to 3 years from the date of membership	For period of membership	Shred hard copy files, delete data files
Suppliers	7 years after the end of the financial year to which the records relate		Shred hard copy files, delete data files
Advice Casework	7 years from date of last contact		Shred hard copy files, delete data files

Form of Authority for Union Support Service

To whom it may concern,

I hereby authorise the appropriate Union Staff and Officers to undertake casework on my behalf and to communicate with staff of City University London and other appropriate third parties for this purpose.

The following staff should not be contacted:

.....

The following third party organisations should not be contacted:

.....

This includes verbal, written and electronic communications.

Name:

Course:

Year:

Course dates:

Student Status: Current | Leave of absence | Withdrawn | Completed

Signed:

Data Subject Access Request Form for Students and Staff

To whom it may concern,

I, _____ wish to have access to data which the City University London Students' Union has about me in the following categories: (Please tick as appropriate.)

- Employment references
- Disciplinary grievance and capability records
- Health and medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc
- Other information: please list below

.....