Data Protection Policy

Approved by:	Board of Trustees
Date of approval:	5 October 2020
Implementation date:	5 October 2020
Review date *(no later than)**:***	5 October 2021
Responsible for implementation:	Chief Executive
Responsible for interpretation:	Board of Trustees

Data Protection Policy

1.0 Policy Statement

1.1 City, University of London Students' Union (the Union) will collect information from individuals and external organisations in order to facilitate the delivery of its services. A portion of this information will be recorded and maintained and will be considered personal data. This policy will:

(a) Represent the Union's commitment to the proper handling of personal data;
(b) Comply with the Data Protection Act (DPA) 2018 and the European Union's General Data Protection Regulation (GDPR) 2016;
(c) Guard against any breaches of statutory and common law responsibilities on the part of the Union and its affiliates;
(d) Encourage and support a culture of best practise within data protection.

1.2 The Union will act as a data controller under the provisions of the DPA (registration number: Z9743163). Personal data will be held in compliance with the DPA and the GDPR.

1.3 'Personal data' refers to information that identifies a living individual, referred to as a 'data subject'. The Union will hold 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, its activities, goods, and services, and promoting public relations.
(c) Accounts and Records – Keeping accounts, screening, liaising with, and maintaining a record of customers and suppliers, maintaining records of purchases, sales and other transactions, the processing of orders and invoices.
(d) Registration of Members – 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, grants, bursaries, and other benefits.
(g) Fundraising – fundraising in support of the objectives of the Union.

1.4 The Union will process personal information about its members in accordance with the GDPR's principles outlined in GDPR chapter 2. This means the Union will commit to processing data such that processing be:

(a) Fair, lawful, and transparent;
(b) Limited in purposes;
(c) Adequate, relevant and not excessive;
(d) Accurate and up to date;
(e) Necessary and therefore terminated upon the expiry of its necessity;
(f) Compliant with the rights of data subjects;
(g) Secure; and
(h) Restricted in the case of the transfer of data to other nation-states except in the case that the other nation-state is able to evidence adequate adherence

to the data protection principles complied with herein or other sufficient protections are applied.

2.0 Background

2.1 The DPA complements GDPR and defines the legal basis for the processing of personal information relating to living individuals.

2.2 The Union will answer, under legal obligation, any subject access request it receives, where 'subject access request' refers to a request from any individual for confirmation as to whether or not personal data concerning him or her is being processed and access to that data as outlined in GDPR Article 15 and DPA Section 45.

2.3 In compliance with the principle of transparency, the Union will inform data subjects what their personal data will be used for, in particular:

(a) Who the organisation in receipt of data is;
(b) What the organisation will use the information for;
(c) That the individual has the right to be informed via Privacy Notices;
(d) That the individual has the right to rectification of their data;
(e) That the individual has the right to erasure (the right to be forgotten);
(f) That the individual has the right to data portability;
(g) That the individual has the right to object to and restrict processing;
(h) The individual's rights in relation to automated decision making and profiling.

2.4 Any individual with concerns about to the handling of their personal data will be welcome to contact and discuss the issue with the Union.

3.0 Management and Staff Responsibilities

3.1. The Chief Executive Officer will be responsible for the general development of, promotion of and adherence to this policy. The Chief Executive Officer retains ultimate responsibility for compliance by all staff.

3.2 The GDPR does not specify periods for the retention of personal data. The Union will therefore provide a Data Retention Schedule as outlined in Appendix A which details the length for which different kinds of personal data will be retained under this policy.

3.3. Union staff who process personal data will be 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 (Appendix A).

3.4. The Chief Executive will be responsible for ensuring that adequate and appropriate knowledge of the GDPR and the Union's legal obligations is available across the Union. The Union will offer training on the GDPR, maintain a working knowledge of its applications in its daily work, include provisions for and information on staff responsibilities in respect of data protection in staff induction materials and contracts, and make this policy publically available to all its members. The senior leadership team will take a position of proactive development in raising awareness of, handling, and learning from any concerns raised.

3.5. In the event of a data breach, the Chief Executive will be responsible for reporting the breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach. The Chief Executive will keep a record of any actual, suspected, threatened or 'near miss' personal data breaches, regardless of whether a notification is required to be sent to the authorities or not.

3.6. In the event that a personal data breach has occurred and is likely to pose a significant risk to the right and freedoms of data subjects the Chief Executive will be responsible for reporting such a breach to the data subjects concerned, subject to the stipulations in GDPR Article 34 and DPA section 68.

4.0 Student Responsibilities

4.1 As a student member of the Union, you will be expected to ensure that your own personal data as provided to the Union is accurate and up-to-date. The Union will ensure that opportunities to update your records are amply afforded.

4.2 Students employed by the Union on a voluntary basis may come into contact with or process personal data in the course of their roles. If you are volunteering for the Union and recording, handling, or processing personal data of any kind and in any way, please inform the relevant department manager in charge of your activity to ensure your data handling remains compliant with this policy, DPA, and GDPR.

5.0 Data Collection within the Union

5.1 Union staff will be considered consenting to the use of their data upon the commencement of their employment. The data collected includes personal, banking, health, disciplinary and equal opportunities information. If you are a staff member, please inform HR of any changes to information that you have previously provided, for example, changes of address or new information relevant to your employment.

5.2 A confidential reference may be 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 appointment of the data subject to any office; or
(c) The provision, or prospective provision, by the data subject of any service.

Such reference will remain confidential and will be exempt from the subject access provisions in that the subject may not gain access to the reference from the body acting as referee. References will be marked confidential.

References may be accessible to the data subject from a third party. A reference may be accessed from its recipient. The contents of any letters of reference or recommendation written by Union staff will be founded on fact and the viewpoints expressed therein will be justifiable.

5.3. The Union Advice service will process personal data pertaining to its users. The Union Privacy Policy, which is complementary to this policy, will detail the principles by which the Advice service handles data and the legitimate interests the Union has

in processing data under GDPR Article 6(1)(f). Advice Service users consent to the Union contacting third parties and to the processing of sensitive categories of data when they sign a form of authority. Union Advice will operate and publish a separate Confidentiality Policy which outlines the very exceptional circumstances where confidentiality (and therefore data protection) may be breached in respect of the Union's Safeguarding Children and Vulnerable Adults Policy.

5.4 Other Union departments will hold student members' data for the purposes of contacting student members with information which is thought to be relevant, valuable, or useful to them. Such information may, for example, relate to volunteering placements, employment placements and media contacts. Members may exercise the right to opt out of the Union but by joining give their consent to such information being collected. Student members' data will also be collected via the Union website for members joining student groups.

5.5 In most cases the Union will refrain from processing data which includes sensitive personal information as these data can, inadvertently or otherwise, lead to discrimination against the persons of which they are subject.

5.5.1 Where the processing of sensitive personal information is unavoidable, e.g. in the case of health and safety records, for the purpose of elections, or for another purpose for which sensitive personal information is necessary, access will be limited to specific members of staff only. The Union will seek consent from data subjects prior to use of sensitive information if consent is not provided for by the Data Sharing Agreement which stands between the Union and the University.

6.0 Data Sharing, Data Security and Disposal

6.1 In order to prevent unauthorised processing, accidental loss, damage or destruction, the Union's paper records of personal data will be stored in locked filing cabinets. Access to records held electronically on IT drives, applications and servers will be managed by password only.

6.2. Data will be shared across business functions and between staff of the Union only when it is necessary to delivering the services of the Union. Data will be 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 will be transmitted solely over a secure network and the transmission of data via paper, post or independent electronic device will be strongly discouraged. The Union network will be a secure system with fully managed access control, back-up and recovery processes in place, managed by City, University of London.

6.3. Where information which could be used to cause an individual damage or distress (particularly financial or medical information) is held on a laptop or other portable device, the laptop or device in question will be encrypted. The level of protection provided by the encryption will be reviewed and updated periodically to ensure that it is sufficient to protect data stored therein in the case that the device is lost or stolen. Specialist technical advice may be sought by the Union concerning encryption and device protection.

6.4. Data will be retained and disposed of according to need and in conjunction with the Data Records Retention Schedule. At the end of the retention period records will be disposed of and/or destroyed, confidentially where necessary. Manual files will be shredded and electronic records will be deleted from central systems.

6.5 A third party 'Memberships Solutions Limited' ('MSL') will provide a membership management system to store and manage our students' personal information. MSL will be 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. MSL will also be contractually obliged to abide by the DPA and GDPR. The system provider will be subject to change; any future provider will be added to and compliant with this policy.

7.0 Sharing Data Routinely with Other Organisations

7.1 The Union will not be responsible for the management of personal data processed by City, University of London, which is solely responsible for its own compliance with the DPA and GDPR. The University reports to the Information Commissioner as a data controller in its own right and will respond to access requests pertaining to data is holds independently of the Union.

7.2 The Union will share information with the University as necessary to pursue its legitimate interests and ensure the smooth operation of procedures and practices in the interests of students, staff and other individuals connected to the Union. All data will be shared under the conditions of the Data Sharing Agreement which stands between the two parties.

7.3 Under circumstances relating to disciplinary activity both the Union and the University reserve the right to share necessary information in order to enforce disciplinary procedures.

7.4 Disclosures of personal data made will not violate either the GDPR or the rights or freedoms of individuals under this or any other legislation.

7.5 Requests for personal data from 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) may necessitate the release of personal data to the third party. The GDPR 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 to release or not release personal data will belong to the Union.

8.0 Request for Information, erasure and modification

8.1 In fulfilling its duties in response to a Subject Access Request, the Union may seek proof of the requestor's identity and any further information required to locate the personal data requested.

8.2 The Union's senior leadership team will supply any data pertinent to a data subject which they hold in the event of a subject access request.

8.3 If you wish to make a subject access request to the Union, you may do so by completing the attached form at Appendix 3 and submitting it to the Union following the instructions contained therein.

8.4 The Union will answer a legitimate subject access request within 30 days as stipulated in the DPA and GDPR.

8.5 The Union will intermittently process personal information to improve offers and services and to enhance the student experience. The Union may, on such occasions, make use of profiling or automated decision making based on student information it already holds (e.g., society membership) or information shared by the University (e.g., department enrolment). If you wish to object to the holding and processing of personal information on an automated basis for the improvement of Union offers and services, you may contact the Union at: studentsunion@city.ac.uk.

If there remains a legal basis for such automated processing of personal data, then the Union may continue to do so, but will offer you (the data subject) an explanation of the processing and the opportunity to challenge it.

8.6 If you wish to request the destruction or erasure of personal information held by the Union, you may do so by contacting the Union at: studentsunion@city.ac.uk.

8.7 If legitimate reasons for the Union to preserve a data subject's personal information (e.g., criminal investigation) persist, the Union will do so even if requested otherwise. Upon the expiry of legitimate purposes, the Union will do its utmost to honour further requests for the destruction of personal data from data subjects exercising their right to be forgotten.

8.8 If you request the destruction of records of your personal data but this data has been shared with the Union by the University, the Union will not be able to remove such data from University systems. You may request the removal of such information from City, University of London systems by contacting the University Registry Department. (020 7040 8321, registry@city.ac.uk).

8.9 Data that the Union holds will not be made available under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 and the Union will not be considered a 'public authority' under the terms defined by either of these acts.

8.10 Records which the University holds about the Union, including communications with the Union and information provided to the University by the Union, will be subject to disclosure through the Freedom of Information Act and the Environmental Information Regulations, and may be requested through the University, which will be considered a 'public authority'.

9.0 Marketing and Communications

9.1 The Union will use data shared by the University to contact its members for the purpose of promoting the services and offers of the Union and its affiliates, subject to the consent of the student members.

9.2 If you wish not to receive these communications, you may opt out at any time. The Union will include this facility in all its communications. The Union also provides facility for opting out of communications on its website, where a member may alter their contact preferences at any time. Communications will not contain information outside reasonable expectations for the relationship between the Union and its members.

10.0 Data Breach

10.1 In the event of a data breach, staff members will be aware of and enact appropriate measures to guard against further breach and address any compromises of personal data as stipulated in GDPR and DPA. Breaches will be reported to the Data Protection Officer, who will be responsible for completing the necessary procedures. The Union's security measures to guard against data breach are detailed in section 6.0 above.

11.0 Complaints

11.1 If you are concerned about any aspect of the management of personal data at the Union you are welcome to raise your concerns, which will be addressed by the Union in a fair and equal way. Please register any of your complaints with the Chief Executive. If you are not satisfied that their complaint has been suitably dealt with, please contact the Chair of the Union Trustee Board.

11.2 If you feel that you are being denied access to personal information to which you are entitled, or feel that your information has not been handled according to the principles laid out in this policy, the GDPR, and DPA, the Union advises you contact the Information Commissioners Office:

The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.
Tel: 01625 545700
Website: www.informationcommissioner.gov.uk

12.0 Duties in Respect of Shared Data

12.1 The Union and University will share data according to the Data Sharing Agreement drawn up between the two. For the avoidance of doubt, some of the duties described therein will be detailed in this policy. For the responsibilities below, the University will be held to a reciprocal expectation.

12.2 The Union will, allowing no more time to elapse than one working day from the point of discovery, notify the University in writing upon becoming aware of any actual or suspected, threatened or 'near miss' Personal Data Breach.

12.3 The Union will, allowing no more time to elapse than twenty eight (28) calendar days from a request from the University or allowing no more time to elapse than 1 working days' notice from the University in the event of a Personal Data Breach, allow its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the University.

12.4 The Union will, allowing no more time to elapse than two working days, notify the University following its receipt of any Data Subject Request or Regulator Correspondence requesting access to, or information concerning shared Personal Data.

12.5 The Union will, allowing no more time to elapse than one working day, notify the University of any claim made by a Data Subject in relation to the Processing of shared Personal Data.

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	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.

I would like to request the following staff not be contacted:

……

I would like to request the following third-parties / organisations 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

Please complete this form and submit it to the Chief Executive of the Union.

Please attach a proof of identification (such as passport, driver's licence or student Identity Card).

To whom it may concern,

I, _____ wish to request 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

……..