CHRIST CHURCH
STUDENTS' UNION

'to better student life and enrich student experiences'

DATA PROTECTION POLICY

Officer Champions	Students' Union President President (Development)
Staff Champions	Head of Business & Development Chief Executive Officer
Approval bodies and date passed	Board of Trustees, 26th June 2020
To be reviewed by	June 2023

1. Introduction

a. Christ Church Students' Union ('the Union') is fully committed to compliance with all data protection regulations and obligations in relation to the management and processing of Personal Data.

b. In order to operate effectively the Union has to collect and use information about the people with whom it works. This may include members of the Union, current, past and prospective employees, clients, customers, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

c. This Policy is intended to serve as general guidance for staff and officers in implementing the letter and spirit of the provisions and principles of data protection and management legislation. The Union will therefore follow procedures which aim to ensure that all members, elected officers, employees, contractors, agents, consultants, or other partners of the Union who have access to any Personal Data held by or on behalf of the Union, are fully aware of and abide by their duties under data protection legislation.

d. This Policy is intended to complement existing Canterbury Christ Church University policies and procedures.

e. The Union is registered with the Information Commissioner's Office, registration number - Z1111670.

2. Definitions

a. Personal Data - data which relates to a living individual who can be identified from the data, or from the data and other information about the individual which is in the possession of or is likely to come into the possession of the Data Controller. Personal Data includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

b. Personal Sensitive Data - personal data relating to racial or ethnic origins, political opinions, religious beliefs, union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences and criminal proceedings.

c. Data Controller - a person or organisation who determines the purposes for which and the manner in which any personal data, are, or are to be, processed.

d. Data Processor - any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

e. Data Subject - a living individual who is the subject of the Personal Data.

f. Processing - the obtaining, recording, holding, organizing, combining, altering, retrieving, consulting, disclosing, disseminating, deleting, destroying or otherwise using the data.

g. Third Party - any person other than a Data Subject or the Data Controller or any Data Processor or other person authorised to process data for the Data Controller or Data Processor.

h. In this policy 'website' means CCSU at www.ccsu.co.uk which is provided by Membership Solutions Limited (MSL).

3. Principles, Processing and Background Information

a. The Union understands and places great importance on the General Data Protection Regulation. This document, alongside the Union's privacy notices, outlines how the Union complies with this legalisation.

b. This Policy refers to both electronic and physical data the Union controls and processes. For more information on the safeguards the Union has in place for each type of data please refer to Appendix A.

c. The Union shares personal data with the following third parties and has undertaken due diligence to ensure such organisations have appropriate data protection policies, procedures and security arrangements in place and are compliant with data protection legislation:
   i. Canterbury Christ Church University;
   ii. Burgess Hodgson - appointed external accounting specialists who facilitate bookkeeping, VAT returns, management accounts, reporting and year end compliance; and
   iii. Kent Union - whom we work with for the provision of representation and opportunities for Canterbury Christ Church University students and Kent and Medway Medical School students.

d. The Union may use other organisations, such as mailing houses, as a data processor in order to deliver a service or communication message. In the event of this, the Union will enter into a data processing agreement with such organisations, on the terms that data can only be used to administer the project specified and that all data will be destroyed following this.

e. In relation to email communication we follow the following processes and rules:
   i. Sending emails concerning representation, research, and membership to current students at Canterbury Christ Church University that have agreed for their data to be shared with the Union by the virtue of the Union's obligations under the 1994 Education Act.
   ii. Sending emails to current students at Canterbury Christ Church University surrounding non-representational Union services and activities where the student has freely given express consent for the Union to do so. Such students can change their consent at any time by opting out through a link provided in each email.
   iii. Sending emails to website guest account holders where the guest has freely given express consent for the Union to do. Such guests can change their consent at any time by opting out through a link provided in each email..
   iv. Sending marketing emails on behalf of carefully selected external third parties where individuals have freely given express consent for us to do. Such individuals can change their consent at any time by opting out through a link provided in each email.

f. Student Committee Members that have access to personal data will do so on the provision of them agreeing to a clear data protection agreement and after adequate training.

g. Student Committee Members will only have access to data for groups that they have been elected to manage.

4. Role of the Data Protection Champion

a. The Head of Business & Development is the designated Data Protection Champion. They are responsible for ensuring this Policy and associated Procedures are implemented and will have overall responsibility for:

i. The provision of data protection training for staff and officers within the Union;
ii. The development of best practice guidelines;
iii. Carrying out compliance checks to ensure adherence to this Policy and data protection legislation; and
iv. Reporting any data protection breaches to the relevant internal and external bodies, including the Information Commissioner.

b. The Data Protection Champion can be contacted via data@ccsu.co.uk.

5. Responsibilities of staff, officers, and other parties

a. All staff and officers within the Union will be made aware of their data handling responsibilities, and take steps to ensure data is kept secure at all times against unauthorised or unlawful loss or disclosure. In particular staff and officers will ensure that:
   i. Paper files and other records or documents containing Personal Data are kept in a secure environment;
   ii. Personal Data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
   iii. Individual passwords should be such that they are not easily compromised; and
   iv. Any incidence, or suspected incidence, of a data breach is reported to the Data Protection Champion without delay.

b. All contractors, consultants, partners or other agents of the Union must:
   i. Ensure that they and all of their staff who have access to Personal Data held or processed for or on behalf of the Union, are aware of this Policy and are fully trained in and are aware of their duties and responsibilities for data protection.
   ii. Any breach will be deemed as being a breach of any contract between the Union and that individual, company, partner or firm;
   iii. Allow data protection audits by the Union of data held on its behalf if requested;
   iv. Indemnify the Union against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

c. All contractors who are users of personal information supplied by the Union will be required to confirm that they will abide by the requirements of the DPA and GDPR with regard to information supplied by the Union.

6. Data We Hold

a. Data from Canterbury Christ Church University surrounding students' personal details are securely transferred into the Union's MSL database in line with the data sharing agreement between **Christ Church Students' Union and Canterbury Christ Church University**. In addition to the data received from Canterbury Christ Church University, the Union records online student behaviour such as purchase history and

any additional data a student directly supplies such as event and membership questions.

b. For guest website accounts, the personal data provided during the registration process, records of online behaviour such as purchase history, and any additional data the individual directly supplies such as event and membership questions.

c. If students at the University give us consent during their website account activation, we may use profiling and screening techniques to ensure communications are relevant to them which involves placing students within a student segment based upon the answers they give to a series of profiling questions. When building a profile, we may analyse geographic, demographic, and other information relating to the student in order to better understand their interests and preferences in order to contact them with the most relevant communications.

d. The Union does not hold University passwords, as website 'logins' are processed through the single sign on process administered by the University.

e. The Union does not hold any bank account or credit debit card details except those of our staff members, student leaders, and student group members for the purposes of expense payments and for suppliers used to fulfil invoices.

f. The Union may, from time to time, collect additional data via online forms and will only use the data collected from these forms to administer the activity or service we are requesting the information for.

g. The Union's Data Retention Schedule is detailed in Appendix Two.

7. Cookies and Tracking Records

a. Cookies are small text files that are stored on a computer when a user visits a website when cookies are enabled. The Union may use cookies to help identify a user's computer to tailor the user experience, and track the purchase process. Users can disable any cookies already stored on their computer, but these may reduce website functionality.

b. The Union will track and log the following to ensure GDPR compliance:
   i. Actions in relation to compliance with the Unions retention of data;
   ii. Logs of data transfer from the University to the Union'
   iii. Information on new data processing activities;
   iv. Actions undertaken requested by an individual; and
   v. Analysis of website registrations.

8. Data Security

a. The Union ensures data is stored in secure databases and servers that adhere to industry standard security arrangements and are ideally located within the European Economic Area. Where the Union uses providers and servers located outside of the

European Economic Area it will ensure it meets the conditions under the General Data Protection Regulation (GDPR).

b. The importance of security for all personally identifiable information associated with our users is of utmost concern to us. The Union takes technical, contractual, administrative, and physical steps to protect all of the user information held. Despite this, the Union and individuals who submit data to the Union, acknowledge and accept that no system can be guaranteed to be 100% secure.

c. It is important that all users protect against unauthorised access to their password and to their computer, and take adequate steps to secure their devices from malicious activity and software. Website users should make sure they log out when using a shared computer and take steps to make sure their personal information has not been stored by the computer and or the network connected to it.

9. Breach Management

a. The Union will respond to a suspected data breach or breach through the following step by step process:
   i. Any breach or suspected breach will be immediately secured to prevent data leak or further data leak.
   ii. An investigation will be initiated by the Data Protection Champion, the University will be informed, and consideration will be taken as to whether the breach is reportable to the Information Commissioner's Office (ICO).
   iii. Any individual affected by the breach will be contacted and any action they can/should take will be explained to them.
   iv. Recommendations will be made to the Leadership Team and Board of Trustees on how such an occurrence can be avoided in the future.

10. Request For Information Held and Complaints

a. Should a data subject wish to request the information the Union holds about them they can do so in writing to comms@ccsu.co.uk. Information will be provided free of charge for reasonable requests upon the satisfactory obtaining of identification.

b. If the Data Subject believes that their Personal Data is inaccurate, out-of-date, held unnecessarily or is offensive, they have the right to have the information rectified, blocked, erased or destroyed.

c. The Data Subject also has the right to insist that the Union ceases to process their Personal Data if such processing is causing, or is likely to cause, unwarranted substantial damage or substantial stress to them or to another.

d. The Data Subject may also have a right to compensation if it can be proven that damage or distress has been caused.

11. Areas of Responsibility

a. The table in Appendix One outlines areas of responsibilities for each of the different areas of main data capturing and processing the Union undertakes.

12. Review

a. This Policy will be reviewed as a minimum every two calendar years or in the event of a data related incident or breach.

Appendix One: Data and Access Table

Area	Data	Responsibility	Accessible To	Safeguarding
Website Database	As described in the Union's privacy notices	Head of Business & Development	All Union staff, sabbaticals, and volunteer officers after adequate training	Database secured by MSL, passwords secured by the University, online data protection training
Online forms	Collected for a specific purpose such as market research	Head of Business & Development	All employees with access to forms relevant to their role	Database secured by Google, passwords secured by the University, online data protection training
Student Groups	Membership details and contact emails	Head of Engagement & Deputy CEO	Elected student leaders restricted to the area of election	Database secured by MSL, passwords secured by the University, online data protection training, specific training to all student group leaders to ensure compliance, specific data protection agreements before access is granted
Advice Service	Case notes and client personal details	Advice & Projects Coordinator and Head of Engagement and Deputy CEO	Advise Service Staff	Database secured by MSL, passwords secured by the University, online data protection training, informed consent process before data is captured, Advise service standards, Policy and Procedures, specific training and CPD
Democracy	Voting records and candidate personal information	Head of Engagement and Deputy CEO	All Union staff	Online data protection training Data protection agreement and data storage policy Specific website training upon induction
Finance	Financial records, statements, staff expenses, and bank account details	Head of Business & Development	All Union staff, sabbaticals	Held in a secure environment Financial procedures and processes Specific training upon induction
Human Resources	Application details, references,	Chief Executive Officer	Management Team	Application consent process Explicit consent upon form collection Employee privacy notice Online data protection

	employee personal details and HR records			training. Data protection agreement, and data storage policy
Marketing	Communication preferences	Head of Business & Development	Communications Team	Digital opt in and out solution.
Staff email accounts	Emails which may include personal information	All employees with an email account	All employees with an email account	Database and passwords secured by Google (CCSU emails), database secured by CCCU/ Microsoft (CCCU emails), online data protection training, IT usage policies, staff training

Appendix Two: Data Retention Schedule

Description of the data	Retention period	Reason for retention period	Action following end of 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	6 years from the end of employment	Provision of references and limitation period for litigation	Shred hard copy files, delete data files
Licensed trade barrings	Life	Enforcement and safety	Shred hard copy files, delete data files
Membership information, including society / sports / volunteers / student media	Up to 3 years from the date of membership expiry	Reporting of engagement and trend analysis	Shred hard copy files, delete data files
Suppliers	7 years after the end of the financial year to which the records relate	Best practice	Shred hard copy files, delete data files
Advice Casework	Up to 3 years from the date of membership expiry	To allow Data Subject access for the purposes of appeals	Shred hard copy files, delete data files
Complaints log	Up to 3 years from the date of the complaint	Reporting of complaints and trend analysis	Shred hard copy files, delete data files
Disciplinary log regarding students	Up to 3 years from the date of membership expiry	Reporting of complaints and trend analysis	Shred hard copy files, delete data files