CHRIST CHURCH
STUDENTS' UNION

'to better student life and enrich students' experiences'

DATA PROTECTION POLICY

Officer Champions	Students' Union President President (Engagement & Sports)
Staff Champions	Head of Business & Development Chief Executive Officer
Approval bodies and date passed	Board of Trustees, 21 January 2022
To be reviewed by	January 2024

[Introduction](#)

[Definitions](#)

[Principles, processing, and background information](#)

[Data Protection Champion](#)

[Responsibilities of staff, elected officers, and other parties](#)

[Data we hold](#)

[Cookies and tracking records](#)

[Data security](#)

[Breach management](#)

[Subject access requests and complaints](#)

[Areas of responsibility](#)

[Review](#)

[Related Documents](#)

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 collects and uses information about the people who work for us, and those who we work on behalf of, and stakeholders who enable us to meet our mission. This Policy outlines in plain language how we use data, what data we hold, and how we take measures to ensure the data we hold is kept securely and safely. Please see the Union's Data Collection, Storage and Retention Schedule for more information.

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. The Data Controller is Christ Church Students' Union. The Union is registered with the Information Commissioner's Office, registration number - Z1111670.

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 Protection Act 2018 - the Data Protection Act 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR. The UK GDPR is the UK General Data Protection Regulation is a UK law which came into effect on 1 January 2021. It sets out the key principles, rights, and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies. It is based on the EU GDPR (General Data Protection Regulation (EU), which applied in the UK before that date, with some changes to make it work more effectively in a UK context:
    i. The right to be informed about what data is being held about you and how it is processed and managed;
    ii. The right of access to data that is held about you;
    iii. The right to rectification if the data that is held about you is inaccurate or incomplete;
    iv. The right to erasure of the data we hold upon you which is also known as the right to be forgotten;
    v. To request the right of erasure;
    vi. The right to restrict processing of the data we hold upon you. This means not deleting the data we hold upon you but placing a certain restriction or total restrictions on how we process it;
    vii. The right to object to the way your data is being held, processed or managed; and
    viii. Rights in relation to automated decision making and profiling.

    Should you wish to exercise any of these rights or if you have a question or concern surrounding your data please complete the online data subject request from here.

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

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

h. 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.

i. In this policy 'website' means the Union's online presence 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 Data Protection Act 2018, and the UK GDPR. This document, alongside the Union's privacy notices and the Data Collection, Storage, Sharing, Retention, and Responsibility Matrix outlines how the Union complies with this legalisation.

b. This Policy refers to both electronic and physical data the Union controls and processes.

c. Where the Union shares personal data with third parties we will always have a legal basis to do so and will undertake due diligence to ensure the organisations have appropriate data protection policies, procedures, and security arrangements in place and are compliant with data protection legislation.

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. The Union's Data Collection, Storage, Sharing, Retention, and Responsibility Matrix details the basis and method of data collection, storage, use, and deletion.

4. Data Protection Champion

a. The Head of Business & Development, Chi Lau, 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. Data collection, handling, storage, and security;
   ii. The provision of data protection training for staff and elected officers within the Union;
   iii. The development of best practice guidelines;
   iv. Carrying out compliance checks to ensure adherence to this Policy and data protection legislation; and
   v. 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, elected officers, and other parties

a. All staff and elected officers within the Union will be made aware of their data handling and retention responsibilities, and take steps to ensure data is kept secure at all times against unauthorised or unlawful loss or disclosure.

b. Staff and elected officers shall only be given access to the data that is reasonably necessary for them to fulfil the role they have been employed or elected to conduct. Before permitted access, staff and elected officers shall undergo training sufficient to their role and data access and handling responsibilities.

c. In particular staff and elected 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 and the use two factor authentication, where possible, will be recommended;
   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.

d. 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.

e. 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 Data Protection Act 2018.

f. The Union's Data Collection, Storage, Sharing, Retention, and Responsibility Matrix details the responsibilities of staff and elected officers concerning the data we hold.

6. Data we hold

a. Data from Canterbury Christ Church University concerning 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, memberships, and any additional data a student directly supplies such as data given to the Advice Centre for the purpose of advocacy.

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 enrolment with the University or upon their Union 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. Students are able to opt-out of such profiling, or to request their profile be reviewed by a member of staff.

d. The Union does not have access to, or hold, a student member's University password, 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 to process payment on www.ccsu.co.uk. The Union does collect and store financial information of staff members and students 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. The purpose of this data collection will be detailed in the form.

g. The Union's Data Collection, Storage, Sharing, Retention, and Responsibility Matrix details the data we obtain, store, and utilise; including the method of obtention and legal basis for doing so.

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 a purchase process. Users can disable any cookies already stored on their computer, but these may reduce website functionality.

8. Data security

a. The importance of security for all personally identifiable information associated with our staff, members, users, and associates 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.

b. The Union ensures that physical data is secured in locked environments when not being used. The Union ensures that electronic data is stored in secure databases and servers that adhere to industry standard security arrangements. These servers may be located inside or outside the United Kingdom. The Union's Data Collection, Storage, Sharing, Retention, and Responsibility Matrix details the storage locations of the data we hold.

c. It is important that all users protect against unauthorised access to their email accounts and password(s) to their internet enabled devices, and take adequate steps to secure their devices from malicious activity and software. Particular care should be taken when using devices that are shared with others.

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. Subject access requests and complaints

a. Should a data subject wish to request the information the Union holds about them they can do so in writing to data@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 Union's Data Collection, Storage, Sharing, Retention, and Responsibility Matrix details the respective responsibilities on the parties involved concerning data collection, security, and retention.

12. Review

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

Related Documents

- Data Collection, Storage, Sharing, Retention, and Responsibility Matrix
- Guest Privacy Notice
- Staff Privacy Notice
- Student Privacy Notice
- Supplier Privacy Notice