CHRIST CHURCH
STUDENTS' UNION

'to better student life and enrich student experiences'

DATA PROTECTION POLICY

Officer Champions	Students' Union President President (Education & Wellbeing)
Staff Champions	Managing Director Finance Manager & Company Secretary
Approval bodies and date passed	Board of Trustees, 23rd June 2017
To be reviewed by	June 2020

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. 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.

2. Policy statement

a. 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.

b. The Union regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence with whom it carries out business. This Policy details how the Union will comply with the two acts of data protection legislation relevant to the Union:

i. The Data Protection Act 1998 (DPA); and
ii. The General Data Protection Regulations 2018 (GDPR).

c. This Policy is intended to complement existing Canterbury Christ Church University policies and procedures.
d. The Finance Manager and Company Secretary is the designated Data Protection Officer and has responsibility for the Data Protection Policy.
e. The Union is registered the the Information Commissioner's Office, registration number - Z1111670.

3. Definitions

a. Personal Data

i. 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

i. 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

i. 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

i. Any person (other than an employee of the data controller) who processes the data on behalf of the data controller, (described in the 1984 Act as a computer bureau).

e. Data Subject

i. A living individual who is the subject of the Personal Data.

f. Processing

i. The obtaining, recording, holding, organizing, combining, altering, retrieving, consulting, disclosing, disseminating, deleting, destroying or otherwise using the data.

g. Third Party

i. 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.

4. Principles of data protection

a. The DPA stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable. The Principles require that personal information shall:

i. Be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
ii. Be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purposes;
iii. Be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
iv. Be accurate and where necessary, kept up to date;
v. Not be kept for longer than is necessary for that purposes;
vi. Be processed in accordance with the rights of data subjects under the Act;
vii. Be kept secure i.e. protected by an appropriate degree of security;
viii. Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

b. The DPA provides conditions for the processing of any Personal Data. It also makes a distinction between Personal Data and Sensitive Personal Data.

5. Handling of data

a. The Union will through appropriate management and the use of strict criteria and controls:

i. Observe fully conditions regarding the fair collection and use of personal information;
ii. Meet its legal obligations to specify the purpose for which information is used;
iii. Collect and process appropriate information and only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;
iv. Ensure the quality of information used;
v. Apply strict checks to determine the length of time information is held;
vi. Take appropriate technical and organisational security measures to safeguard personal information;
vii. Ensure that personal information is not transferred abroad without suitable safeguards; and
viii. Ensure that the rights of people about whom the information is held can be fully exercised under the DPA. These include:

1. The right to be informed that processing is being undertaken;

2. The right of access to one's personal information within the statutory 40 days;
3. The right to prevent processing in certain circumstances; and
4. The right to correct, rectify, block or erase information regarded as wrong information.

b. In addition, the Union will ensure that:

i. There is someone with specific responsibility for data protection in the organisation;
ii. Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
iii. Everyone managing and handling personal information is appropriately trained to do so;
iv. Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
v. Queries about handling personal information are dealt with promptly and courteously;
vi. Methods of handling personal information are regularly assessed and evaluated; and
vii. Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of Personal Data will be in compliance with approved procedures.

6. Responsibilities of officers, staff 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 that Personal 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 and Sensitive 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 Officer 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; and
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.

7. Data collected, stored and processed by the Union

a. The Union holds a range of information on individuals, mostly students of the University, Staff of the Union and contractors supplying the Union. This is collected and stored in a variety of ways, detailed below (this list is not intended to be exhaustive).

b. Student Members of the Union:
   i. Personal Data concerning demographics and course, collected by the University upon enrolment, where consent is given, and transferred to the Union via the GDPR compliant Data Transfer Agreement (available on the Union's website). Digital record.
   ii. Personal Data collected by the Union, with the consent of the individual as detailed at the point of collection. E.g. from elections candidates, for volunteering projects or during surveys. Digital record.
   iii. Personal Data and potentially Sensitive Personal Data concerning students given freely to the Advice Service (e.g. medical declarations or disclosures of criminal convictions). The recording of Sensitive Personal Data is discouraged but is sometimes necessary to act in the best interest of the Client. Only the Advice and Campaigns Coordinator and the Membership Services Manager has access to the Advice Centre Records (see the Union's **Advice Centre Policy and Procedures**). Digital and paper record.

c. Staff Members of the Union:
   i. Personal Data concerning demographics, and consent is given as part of the new starter process. As Union staff are employed by the University, Sensitive Personal Data is stored by the University. Digital and paper record.

d. Contractors supplying the Union:
   i. Financial records for the purposes of payment, invoicing etc, collected with consent at the point of contract / transaction. Digital and paper record.

8. Security of data

a. Union staff and officers responsible for processing Personal Data must ensure that it is kept securely to avoid unauthorised access and only disclose to those authorised to receive it.

b. Digital records:
   i. Care must be taken to ensure that PC's on which Personal Data is viewed are not visible to unauthorised persons, especially in public places;
   ii. Screens showing personal data should not be left unattended and unlocked;
   iii. University passwords are required to be changed every 6 months, and it is recommended that Google Drive passwords are changed at this frequency also, and are not the same password as for University login for added security; and
   iv. The Google Drive has the facility to shared files and data outside the organisation, but doing this for Personal Data is prohibited unless express consent has been obtained from the Data Subject(s).

c. Paper records:
   i. In the case of manual data, files containing personal data should be kept in locked storage cabinets when not in use;
   ii. Files should not be left on desks unattended; and
   iii. The Union provides facilities for the confidential destruction of limited amounts of paper documents within the offices in Canterbury, Medway and Broadstairs. If a significant number of documents require secure destruction (e.g. annual financial records at the expiry of the required retention period) the Union may utilise the University's arrangements for this service.

9. Sharing data routinely with other organisations

a. The Union reserves the right to share information with Data Processors as necessary to pursue its legitimate interests, or to ensure the smooth operation of procedures and practices in the interests of beneficiaries.
b. Disclosure of Personal Data is always made in accordance with the DPA and GDPR and never prejudices an individual's rights or freedoms.

10. Role of the Data Protection Officer

a. The Finance Manager & Company Secretary is the designated Data Protection Officer. They are responsible for ensuring this Policy is implemented and will have overall responsibility for:
   i. The provision of data protection training for staff and officers within the Union;
   ii. For the development of best practice guidelines;
   iii. For carrying out compliance checks to ensure adherence to this Policy and data protection legislation; and
   iv. For reporting any data protection breaches to the relevant internal and external bodies, including the Information Commissioner.

11. Right of access by the Data Subject

a. The DPA gives Data Subjects the right to access to their Personal Data held by the Union. A request must be made to the Data Protection Officer via email (hello@ccsu.co.uk), and a £10 administrative fee paid. This entitles the individual to be told if the Union is:

   i. Processing that individual's Personal Data;
   ii. The purposes for which they are being processed;
   iii. To whom they are or may be disclosed; and
   iv. To receive this information in an accessible manner which includes a copy of their Personal Data.

b. The Union must ensure that it has proof of the identity of the requestor to prevent an unlawful disclosure and is required to respond within 40 calendar days of receipt of the request and the fee.

12. Complaints by a Data Subject

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

13. Retention schedule

a. The DPA does not specify periods for the retention of Personal Data. Instead, Union management is responsible for how long Personal Data should be retained, taking into account the Data Protection Principles, business needs and any professional guidelines. Overleaf is the retention schedule for the Union.

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