

Worcester Students' Union (WSU) Privacy Statement

Introduction

Worcester Students' Union ("The Union" or we" or "WSU") is a charitable organisation (no. 1145192) whose registered address is Henwick Grove, Worcester, WR2 6AJ. Worcester Students' Union Trading Company Ltd is the registered trading company for Worcester Students' Union.

Our primary purpose is the advancement of education of students at the University of Worcester through the delivery of our charitable objects.

We have approximately 35 employed staff (both core staff and student staff) and around 350 volunteers based from the above premises. The Union stores and processes some of its data remotely through:

- University of Worcester managed servers (O Drive and N Drive)
- One Drive
- Membership Solutions Ltd (MSL) servers
- Committee member and volunteer personal laptops

All of the above are data processors to the Union as data controller. We have GDPR compliant processor contracts in place with all of the above named parties. All processors undertake to keep the data within the EEA or are compliant and certified under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

The Union has sought legal and professional advice on matters of the GDPR from employment law specialists at TLT LLP and the Information Commissioner's Office. This document and the processes established in managing our data compliance has had oversight and guidance from the Union's Trustee Board.

Policy Statement

1. The Union intends to comply with GDPR or the same as subsequently enacted into UK domestic law at Brexit.
2. We will therefore:
 - a. Only process as much personal data as is necessary for our legitimate administration and the services we supply.
 - b. Only hold such data for so long as necessary for those legitimate purposes. We have an agreed retention schedule detailing what we deem to be appropriate periods to hold data for the varied Union activities and purposes. As in most cases this is only archived data, not sensitive, not dangerous and will not be used, there seems little risk to data subjects.

- c. Only process such data on grounds for lawful processing provided within Point 6.
 - d. Send or otherwise provide appropriate notices to those whose personally identifiable information ("Personal Data") is processed by us including our employees, volunteers and individuals or individuals within partners who supply us with goods or services.
 - e. Not engage in direct marketing to clients or members otherwise than in accordance with the relevant legislation and guidance from the ICO.
 - f. Utilise appropriate organisational and technical measures to ensure that Personal Data processed by us is kept secure.
 - g. Where we use third party data processors, we will choose them carefully with a view to their data security and compliance with GDPR and have GDPR compliant contracts with them.
 - h. Not transfer Personal Data to recipients located outside the European Economic Area and the UK without confirmation from our Data Protection Officer and the University's Head of Information Assurance that such transfer is lawful.
 - i. Review this document on an annual basis so that it remains an accurate record of our data processing activities and policies.
3. The Chief Executive is appointed as our Data Protection Officer.
4. Following advice, we have concluded that GDPR is not intended to require us to treat employees of our current or prospective partners, sponsors, and suppliers whose contact details we are required to use for dealing with those organisations, nor individuals who contact us intending to engage in correspondence with us, as data subjects to whom we should send notices pursuant to Articles 13 and 14 merely because we hold and use those contact details in connection with our dealings with them or their employers, or keep copies of such communications, as the effect of such interpretation would be disproportionate.
5. We conclude that where we hold and process such personal data for the purposes of direct marketing to those individuals' employers we should, unless guidance from the ICO says otherwise, either:
 - a. obtain consent to that direct marketing from the individuals and send the notices required by Points 13 and 14 to the individuals; or
 - b. be satisfied that we have a legitimate interest in holding that Personal Data and using it for that purpose.
6. Following advice, we have concluded that when employees', trustees' or members' data is shared with our bank, pension provider, insurance provider, HMRC, BUCS, National Governing Bodies, volunteering organisations, and the Charity Commission, these organisations are neither our processor nor joint controller of the

data concerned. This is because the data is being provided for their own use as they see fit to provide a service to us and/or benefits to our employees, trustees and members. We will, where possible, however, require contracts with them containing confidentiality obligations in respect of that data and other data that they create relating to our employees, members or customers in the context of the work they are doing.

7. In partnership with the University of Worcester, who collect our membership data as part of their enrolment process and responsibilities for enabling the Education Act, we have determined that we are a joint controller of this data. Through being a joint controller, we are able to share membership data as appropriate between both organisations.

8. Following advice from the Information Commissioner's Office, we have concluded that in joining a specific club or society which is linked to special categories of personal data (such as LGBT+, Labour Students or ISOC) it would only be an assumption that the person was providing information about their sexuality, political or religious beliefs and as such would not come under the special category of personal data.

WSU's Data Records Processing and Retention Schedule

In line with our data sharing agreement with the University of Worcester, our records processing and retention schedule adheres to the University's corresponding policies.

Definitions used:

Archival value

Some records may have archival/historic value and should be retained. The University has a long term storage facility which can be used for archive records. Please contact infoassurance@worc.ac.uk

Review

For some records deletion/destruction at the end of a specific period needs to be carefully considered especially if there may be archival/historic value to the record. Once a review has been undertaken if there is no merit in retaining the record it should be deleted or if it is retained a future review date should be noted.

While current (ie whilst still a student registered at the University of Worcester or a current employee, Officer or trustee of Worcester Students' Union)

These records will relate to personal data which is dependent on an individual's consent being obtained. The accuracy of the records should be checked on at least an annual basis and consent re-obtained for processing.

Year Created +

In the example Year created + 5 – if the record was created in 2015/16 then it is due for deletion/destruction in 2020/21

1. Full and associate members

Personal data collected:	Student ID, University Email Address, First and Last Name, Nationality, Department (if available), Course, Course Level, Current status e.g. PT or FT, Academic Rep Status , Date of Birth, Student Accommodation Type Where appropriate or necessary for engagement with WSU activities or services or to protect the vital interests of members – DVLA numbers, next of kin details, signature, medical details, postal address, CCTV images
Special categories of data collected:	Gender
Data origination:	University of Worcester, Student Directly
Storage location:	University of Worcester servers - O Drive and N Drive, One Drive, Membership Solutions Ltd (MSL), Advice Pro, Survey Monkey Inc. servers, locked filing cabinet
Identified data usage:	Membership records (sports and societies), advice centre user records, volunteering records, records of attendance at events, purchase history, elections & referenda voting history, complaints and discipline records, democratic engagement history, survey responses and analysis, registered driver details, inbound and outbound payments, refunds, course rep records, research engagement, Ideas Forum engagement, health and safety records, DBS checks (if necessary), medical records (if necessary), pre-event forms, NUS Extra purchases, retail purchases, Student BACS transfer form, health and safety processes e.g. incident or accident forms
Third parties with access:	University of Worcester, National Governing Bodies, BUCS, Membership Solutions Ltd (MSL), National Union of Students (NUS)
Retention period:	Advice cases – Year created + 6 Society or sports team membership – Current + 6 Volunteering registration – Current Elections candidacy – Current Voting history (referenda and elections) – Permanent Survey responses – Year created + 5 Survey analysis - Permanent Complaints and discipline records – Current + 6 Course Rep records - Current Purchasing records – Current Event attendance – Current Event notification forms – 1 year Driver's details – Whilst current DBS checks – Created + 6 months

	CCTV data – as per University Policy (date created + 9 weeks) Financial details /Student BACS transfer form– once payment / refund or ongoing payment period has finished Medical records and next of kin details – once event or trip requiring the information is complete Ideas Forum data – Current Ideas Forum analysis - Permanent Health and Safety forms/records – Year created + 6
--	--

2. Guests of members

Personal data collected:	Full Name, CCTV images
Special categories of data collected:	None
Data origination:	Provided by individual
Storage location:	CCTV Control Units (University), event attendance records, Membership Solutions Ltd (MSL), locked filing cabinet
Identified data usage:	CCTV, Event ticket sales history, inbound and outbound payments, refunds and retail purchase history, health and safety processes e.g. incident or accident forms
Third parties with access:	None
Retention period:	Event attendance forms - 1 year CCTV images – as per University policy (date created + 9 weeks) Health and Safety forms/records – Year created + 6

3. Employees of suppliers, contractors and clients

Personal data collected:	Email Address, Full Name, Business Name, Postal Address, Role Title, Telephone, and Bank Details
Special categories of data collected:	None
Data origination:	Provided by individual
Storage location:	SAGE, Co-operative Bank, Locked Filing Cabinet

Identified data usage:	Client invoices, supplier payments, communications, credit management and fraud prevention, health and safety processes e.g. incident or accident forms
Third parties with access:	NUS Media Local
Retention period:	Data to be kept for the length of the contract + 6 Health and Safety forms/records – Year created + 6

4. Employees of the Union

Personal data collected:	Email Address, Full Name, Telephone, Postal Address, Role Title, Date of Birth, NI Number, Bank Details, P45 / P46, Next of Kin/Emergency contact details, Disciplinary Record, Business Interests, Right to work in UK, Reference Personal Details, For student staff - Course, Year of Study and Student ID During the recruitment process - Email Address, Full Name, Telephone, Postal Address, Date of Birth, Employment and Remuneration History, Reference personal details
Data origination:	Provided by individual
Special categories of data collected:	Gender, Criminal Record and, Ethnicity, Sexuality (for Diversity Monitoring purposes only, including during the recruitment process), Personal Health/ Medical Records once appointed
Storage location:	Locked cabinet, SAGE, Co-operative Bank, O Drive, N Drive
Identified data usage:	Employee administration, recruitment processes and expense claims, payroll, health and Safety processes e.g. incident or accident forms, DBS Checks, (if necessary), HR processes e.g. sick leave, disciplinary or grievance procedures, holiday leave, appraisals, exit interviews etc.
Third parties with access:	HMRC, SAGE, University of Worcester, AEGON, SUSS, NEST, Cooperative Bank
Retention period:	Recruitment records – Created + 6 months (where employment is subject to Visa retain in accordance with UKVI guidance) HR records including medical information, sick leave records, disciplinary or grievance records, appraisals etc. – Current + 6 Holiday leave – Created + 1 Reference for staff – Created + 1 Next of kin/emergency contract details – While current Financial details – While current Payroll – Year created + 6

	HMRC records – 3 years DBS checks – Created + 6 months Health and Safety forms/records – Year created + 6
--	---

4.1 Trustees of the Union

Personal data collected:	Email Address, Full Name, Telephone, Postal Address, Date of Birth, Next of Kin Details, Business Interests, Declaration of Interests Form, bank details, Reference Personal Details During the recruitment process - Email Address, Full Name, Telephone, Postal Address, Date of Birth, Employment and Remuneration History, Reference personal details
Data origination:	Provided by individual
Special categories of data collected:	Gender, Criminal Record and, Ethnicity, Sexuality (for Diversity Monitoring purposes only, including during the recruitment process),
Storage location:	Locked cabinet, O Drive, N Drive
Identified data usage:	Trustee administration, recruitment processes and expense claims health and Safety processes e.g. incident or accident form, DBS checks (if necessary)
Third parties with access:	Charity Commission, Co-operative Bank
Retention period:	Recruitment records - 6 months after not being appointed to a role HR Records – Current + 6 References for trustees – Created + 1 Financial records – While current DBS checks – Created + 6 months Health and Safety forms/records – Year created + 6

5. Data Storage

The Union stores and processes some of its data remotely through:

- University of Worcester managed servers (O & N Drives)
- One Drive (Cloud-based platform)
- Survey Monkey Inc.
- Membership Solutions Ltd (MSL) servers
- Committee member and Part Time Officer personal laptops

All of the above are data processors to the Union as data controller. We have GDPR compliant processor contracts in place with all of the above named parties. All processors undertake to keep the data within the EEA or are compliant and certified under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

6. Organisational and technical measures

We use the following organisational and technical measures to ensure the confidentiality of personal data:

- a. Provisions that employees and volunteers who process data are required to consider the use of lockable filing cabinets, secure storage for archived files and the use of a shredder or confidential waste bin for hard copies of paperwork, file notes, incoming and outgoing letter correspondence containing personal data.
- b. For electronically held data, employees and volunteers who process data are required to use, wherever possible, storage on the University server or cloud-based platforms approved by the University. They must ensure password protection on all files containing personal data, the use of the University's secure platforms for processing data, running up to date antivirus and malware systems, installation of adequate firewalls, the secure destruction or disposal of IT equipment.
- c. Access to the CCTV units and systems are through authorised University personnel only.
- d. Email accounts are individually assigned and not shared with colleagues or third parties. Access to emails are only authorised for third parties for specific purposes by the Data Protection Officer.
- e. The data protection and information security staff handbook provides clear guidance on data sharing, data handling, security breach procedures and disposal of data.
- f. We hold GDPR compliant contracts with all data processors.
- g. All employees and volunteers undertake training in data protection and information security awareness being given authorised access to process data held by the Union.

7. Consent

We do not engage in direct marketing to individuals.

Following guidance from the ICO and a review of the appropriate legislation we have concluded that as our members have purchased through their tuition fees a membership of the Union we do not need consent in communicating through digital means with our members about our charitable activities, events, and services. We believe that as a member there is a legitimate interest in receiving this information. Upon enrolment, there is an opt-out option for all students who do not wish to have their data shared with the Union.

Where the Union is undertaking campaigning, lobbying, or acting as a conduit for commercial, marketing activities (on behalf of third party sponsors) explicit consent shall be obtained.

The Union follows industry guidance relating to research gathering. Where personal data is collected as part of a research exercise this shall be undertaken with the

explicit consent of the individual.

We are aware that consent under GDPR must be freely given, specific, informed and unambiguous given by a statement or a clear affirmative action and that we have to keep a record of each consent obtained for as long as we are using it. We do not currently believe that any of our processing of personal data, except for the sending of specific commercial marketing and research activities, requires data subject consent.

8. Legitimate Interests

Recital 47 of the GDPR reads: *"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller."*

We rely on legitimate interest as justifying much of our processing of Personal Data as we have assessed that the majority of our processing activity would be in the reasonable expectations of those we process data about. Our activities reliant on legitimate interest are as follows:

- a. **Employees and Trustees:** We require the data processing to enable us to be a good employer and pay employees. Whilst they are candidates, we require it to assess them for employment. Employees, trustees and candidates expect us to hold and process that personal data for those purposes. We destroy candidate personal data if the candidate is unsuccessful after 6 weeks of not being appointed.
- b. **Members:** As a membership organisation, processing individual data is central to our service provision. Members are able to opt-out of processing by terminating their membership. To provide a high standard of service and personalise our provision, we record and process data relating to members engagement and communications preferences. We have a data sharing agreement in place with the University of Worcester who refresh our data weekly and daily during enrolment and Elections periods.
- c. **Suppliers, partners and clients:** Our suppliers, partners and customers are not usually individuals so here we are dealing with the identifiable employees of our suppliers and clients who require us to deal with such individuals or self-employed individuals. We require their personal data (email, office address, telephone numbers) to enable us to contact them in the context of their job. If an employee leaves a client or supplier we remove their details from our systems (or we would be communicating with the wrong person). They expect that we will hold their contact details for this purpose.
- d. **Customers:** When individuals purchase products or utilise services through our us, we have access to process this data to administer our contracted duties.

In all the above cases, we believe that we have a legitimate interest in carrying out data processing and that the processing has no significant risk to the rights and freedoms of the individuals concerned.

We will only send marketing information to individuals who have not objected to receiving digital mailings in compliance with our policy. Individuals' consent will be sought and recorded for such mailings.

9. The Education Act

Together with the University of Worcester, we have interpreted that the act requires all University of Worcester students to be members unless they opt-out, which revokes any requirements to receive explicit consent for data processing in relation to the administration of membership.

10. Members

We are satisfied that our activities serve a legitimate interest to our members and do not risk the rights and freedoms of the individuals concerned. We are required to deliver certain services by the Education Act for our members. Our members are informed of our activities upon enrolment with the University.

11. Employees

We are satisfied that we only process employee Personal Data where we have a legitimate interest in so doing and are changing/have changed our contracts of employment to make this clear and include the necessary notices.

We hold medical details and next of kin/emergency contact details in respect of employees. This is authorised under GDPR as the processing is necessary to protect the vital interests of the employee.

12. Notices

We do not believe that GDPR should be interpreted as requiring an Article 13 or Article 14 notice to be sent to every data subject whose personal data we are processing. We do believe that such notices should be sent to:

- Suppliers and clients once engaged with the Students' Union
- Our employees and those going through the recruitment process
- Identifiable employees, members, University staff or attendees of minuted meetings
- Local or national organisations who provide volunteering opportunities for our members

13. Data Processors

We have identified the following parties as data processors:

- University of Worcester- In the provision of managed servers (O&N Drives)
- MSL - in the provision of Students' Union website servers
- SAGE - In the provision of accounting software
- HMRC
- Cunninghams - ePOS provider
- Survey Monkey Inc. (Wufoo and Survey Monkey services)
- Volunteering organisations

The above parties either have a direct contract using the Students' Union model contract or through GDPR compliant terms and conditions of use of service.