Worcester Students' Union (WSU)
Data Protection and Information Security Policy

Contents

1. Introduction

The Union has a duty to obtain, store and retain personal information of its staff, members, trustees, volunteers, suppliers, and other individuals about whom we might hold data, for legitimate purposes only. It will do so in line with the General Data Protection Regulations (GDPR), which came into force in May 2018, and are the primary statutory authority on handling and processing data. WSU is registered with the Information Commissioner's Office (ICO). This policy sets out how WSU will abide by the GDPR and adhere to its responsibilities around protecting personal data.

Data protection is not just the responsibility of management within WSU but of every employee, volunteer, member or contractor handling data collected or administered by WSU who must ensure appropriate use in line with this policy. Any deliberate breach of this policy may lead to disciplinary action being taken under the WSU's staff or membership procedures or even a referral to criminal proceedings. It may, also, result in personal liability for the individual.

Please see Point 8 of WSU's Privacy Notice for more information on what WSU deems to its legitimate interests for handling data.

Any questions or concerns about the interpretation or operation of this policy should be addressed to the Data Protection Officer.

2. Data Protection Officer

Data Protection arrangements are overseen by the nominated Data Protection Officer (DPO) of WSU, who is the Chief Executive. The DPO reports to WSU's Trustee Board and is responsible for:

- Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection or electronic communications regulations or laws;
- Monitoring compliance with the GDPR and other data protection laws, including managing internal activities, ensuring privacy impact assessments re conducted where necessary, ensuring staff are trained, and conducting internal audits;
- Ensuring WSU's risk register is updated and maintained to include data protection processes;
- Being the first point of contact for supervisory authorities and for individuals whose data is processed (employees, members etc.);
- Liaising with the University's Head of Information Assurance for advice and guidance on matters relating to data protection.

The DPO shall be assigned the SUdataprotection@worc.ac.uk email address.

3. Responsibilities

3.1 Students (members), suppliers, contractors and other individuals

Students (our members), suppliers, contractors and other individuals about whom we hold information, must ensure that personal information and data provided to the organisation is up to date and accurate. They must, also, read and understand the relevant terms of engagement with WSU. They must ensure that changes in personal details are updated on the appropriate systems by contacting the relevant member of WSU co-ordinating or overseeing that activity.

As per Point 7 of WSU's Privacy Statement, with regards to our members' data, 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.

WSU will seek consent from other individuals who are not members before they handle, store or process their data for legitimate purposes, which will be recorded. If, at any point, the purpose of holding or processing that data changes, the individuals concerned will be notified and updated consent sought. If consent is not obtained, the individual's details will be deleted and records of the deletion will be documented.

3.2 Student volunteers

Committee members, student representatives, and other student volunteers, may handle limited personal data to administer their activities. They must have completed the relevant data protection training prior to receiving permission to handle any personal data related to WSU activities and must comply with this policy.

Records of volunteer training will be maintained by the Student Engagement Manager. Student volunteers must report any data breaches and respect the right of individuals when handling data, ensuring secure processing procedures.

3.3 Employees (including student staff)

WSU employees must ensure that personal information and data provided to the organisation in the process of employment is up to date and accurate. They must ensure that any changes to their personal details are updated by informing WSU's HR & Admin Co-ordinator.

In the normal course of work, it is likely that staff will process individual personal data and they must do so in line with this policy. Prior to handling data, staff are required to have completed the relevant data protection and information security training. Staff must also maintain a good, current knowledge of data processing best practice through refresher courses and learning available on the Information Commissioner's Office (ICO) website (www.ico.org.uk), and report any concerns to WSU's Data Protection Officer. Records of staff training will be maintained by the HR & Admin Co-ordinator.

Co-ordinators and Managers within the organisation are required to conduct periodic audits (e.g. once per semester) of their relevant areas and IT records to ensure compliance with this Policy and to identify any possible weaknesses in information security, which must be reported to the DPO.

3.4 Management Team

WSU's Management Team are responsible for demonstrating ownership of this policy and for communicating its values and importance across the organisation. They are accountable for this policy, albeit they may delegate aspects of data protection management to other appropriate staff within the organisation.

The Management Team must ensure resources are available to fulfil the requirements of this policy and its associated procedures. It must seek expert advice when necessary, from the University's Head of Information Assurance and/or from the ICO, and report any data breaches as per ICO requirements.

3.5 Trustee Board

As the governing body of WSU, the Trustee Board, has overall accountability for the strategy of the organisation and is responsible for strategic oversight of all matters related to statutory, legal compliance and risk. The Trustee Board shall review the organisation's risk register on at least an annual basis and should seek assurance from the Management Team that effective arrangements are in place around data protection.

4. Compliance

4.1 Respecting Individuals' Rights

The GDPR sets out a series of rights for individuals, as below. WSU employees and volunteers undertaking or planning data processing activities must record how these rights are addressed.

4.1.1 The right to be informed

The right to be informed encompasses WSU's obligation to provide 'fair processing information', usually through a privacy notice. It emphasises the need for transparency over use of personal data. WSU publishes privacy notices at www.worcsu.com/faqs/data_protection. For students, employees, suppliers and contractors these must be referred to at the point of data collection or when processing third party data.

4.1.2 The right of access

Individuals have the right to access their personal data and supplementary information which allows them to be aware of and verify the lawfulness of the processing. Individuals requiring access to the data the Union holds on them must complete a ***Subject Access Request Form***. See Point 4.3 below.

4.1.3 The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. WSU must retain a clear trail of where information has been disclosed to third parties.

WSU must respond within one month of receipt of a ***Data Rectification Form***. Any employees or volunteers receiving a Data Rectification Form must send this to the Data Protection Officer within 5 days of receipt to ensure rectification of the individual's data within the timeframe.

4.1.4 The right to erase

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

A large majority of data WSU processes relates to the delivery of service - individuals must be aware and are informed that erasure of their data will not only mean inability to serve them but if complete erasure from Union records is required then this will result in termination of membership. Individuals should be directed to the ***Data Erasure Request Form*** which should be sent to the Data Protection Officer to coordinate the administration of the erasure within 30 days of the request. Any third parties in prior receipt of that individual's data must also be informed of the erasure, unless it is impossible or involves disproportionate effort to do so.

4.1.5 The right to restrict processing

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, WSU is permitted to store the personal data, but not further process it, an example being members opting out of receiving email communications.

For data processing activities such as email and SMS communications, WSU provides automated opt-out systems which the individual can use to limit our processing. For processes where automated systems are not available, individuals should be directed to the ***Data Restriction and Objection Request Form,*** which should be sent to the Data Protection Officer to coordinate the administration of. As with erasure, restrictions of processing may result in the Union's inability to serve the individual with a specific service or activity, and where third parties have been shared with this data, they must be informed of the restrictions.

4.1.6 The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Individuals can request their data using the ***Subject Access Request Form*** and employees and volunteers should respond to these requests in the same time-frame as the access requests detailed previously.

4.1.7 The right to object

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

4.1.8 Rights in relation to automated decision making and profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. The Union does not make automated decisions about individuals that may be damaging without any form of human intervention.

4.2 Processing special categories of data

WSU will only process special categories of data linked to individuals, such as health data, religious and sexual orientation, with the consent of individuals, except for when the disclosure is to preserve life or for legal purpose. This data may be analysed in broad terms where no direct link to an individual can be made.

4.3 Subject Access Requests (SARs)

As standard, WSU does not charge to comply with SARs and will refuse manifestly unfounded or excessive requests. Any individual or department receiving an SAR must share this with the Data Protection Officer (DPO) within 2 working days. The DPO will respond to the request within one month of initial receipt.

Individuals have the right to access their personal data and supplementary information which allows them to be aware of and verify the lawfulness of the processing. Individuals requiring access to the data the Union holds on them must complete a ***Subject Access Request Form***.

The Union must respond to these requests within one month. Any staff member or volunteer receiving a Subject Access Request Form must send this to the Data Protection Officer within 5 days of receipt to ensure a response within the timeframe.

4.4 Lawful Data Processing

WSU shall only process data within the law. Where a lawful process has been identified, WSU employees and volunteers must make a record of the lawful justification within the relevant privacy notice. Privacy notices will identify the legal basis for processing personal date and will cover:

- What information is being collected;
- Who is collecting it;
- How it is being collected;
- Why it is being collected;
- How will it be used;
- Who will it be shared with and how;
- What the effect will be of this on the individuals concerned;
- If the intended use is likely to cause individuals to object or complain.

4.5 Under '18s

WSU staff and volunteers shall not process data related to any individual under the age of 16. In the unlikely scenario of a requirement to process data of an under 16, the DPO shall be responsible for ensuring the processing is robustly compliant with GDPR standards.

Where the Union is required to process data of a member who is under the age of 18, e.g. a student who is 17 at the time of enrolling at University, it will seek the necessary permissions to do so, in consultation with the University's Head of Information Assurance and in line with University registration procedures.

4.6 Data Breaches

WSU will conduct regular audits to detect data breaches. Where an employee, volunteer or other individual about whom the organisation holds information discovers a data breach, they must report this to the DPO within 24 hours via SUdataprotection@worc.ac.uk

The ICO will be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals, such as discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant disadvantage. Where there is a high risk to individuals' rights and freedoms, they shall also be notified directly.

Further information for WSU employees and volunteers on what to do if they suspect a data breach can be found in WSU's Data Protection Handbook.

4.7 Privacy Impact Assessments /Legitimate Interest Assessments

When planning new data collection or processing, WSU employees are required to conduct Privacy Impact Assessment (PIA) and, where appropriate a Legitimate Interest Assessment (LIA). Further details for WSU employees on when and how to conduct a PIA or LIA can be found in WSU's Data Protection Handbook.

5. Information Security

5.1 Data Storage

Electronically stored personal data must be stored in an encrypted or password protected form to protect against unauthorised access or processing.

Physical representation of data, such as paper forms, will be kept to a minimum and must be stored within locked cupboards and units. WSU's retention schedule will be adhered to and, when no longer needed, e-copies shall be deleted (through liaison with University IT) and paper copies securely destroyed and disposed of.

Access to WSU offices are restricted to WSU staff and access to the Finance office, where the majority of sensitive, personal data will be stored, is further restricted to appropriate members of WSU staff.

Vital records for the purposes of business continuity, payroll, and tax purposes etc., must be protected from loss, destruction or falsification by WSU employees, in accordance with statutory, regulatory, contractual and WSU policy requirements. There will be a central record of all paper and electronic records kept.

WSU will securely maintain a Data Mapping Mastercopy which will detail all of the personal data the organisation holds and for what legitimate purpose, as well as identifying any high risk information (and the enhanced security around such information). This will be reviewed on a regular basis to ensure that personal data collected is accurate, adequate, and relevant and not excessive. Routine weeding will be carried out to remove any records that are no longer needed or are out of date.

It will, also, maintain a Data and Document Retention Schedule detailing how long data must kept for different purposes before being securely deleted or destroyed, and a Decision Log of times it has agreed to share data with a third party.

5.2 IT Systems

WSU has 3 primary platforms for securely storing data on-line – the Cloud-based One Drive, the University of Worcester O:Drive and the University of Worcester N:Drive. Employees and volunteers are required to store data they handle only on one of these platforms.

WSU employees must undertake the University Information Security Awareness Training to ensure sufficient security awareness and comply with University IT policies and procedures, as referred to in the Staff Handbook.

Employees and volunteers must make best attempts to protect their identity by using a strong password and follow the guidance on this from the University's IT department. Account passwords and usernames should not be shared without authorisation from the DPO.

Electronic and digital equipment and media containing information must be secured against theft, loss or unauthorised access when inside and outside of WSU premises. All such equipment must be disposed of according to University IT policy when no longer required. The University's IT policy can be found at

https://www.worcester.ac.uk/informationassurance/content_images/Information_Security_Policy_v_1.1_July_2017.pdf

WSU will liaise with the University's IT department to ensure a regular (e.g. annual) deletion of data from the N and O Drives, which is no longer required for use by WSU.

WSU will liaise with its website provider, Membership Solutions Limited, to ensure an annual deletion of data it no longer needs from the digital platform.

IT records will be backed up by the University, according to their IT policy.

5.3 Data in Transit

Physical e.g. paper copies of data in transit e.g. sports team sheets or event forms, will be the responsibility of agreed team captains or event leads/supervisors. They will be returned to the relevant WSU co-ordinator as soon as practicable after the fixture or event for secure storage and retention, according to WSU's retention schedule. In the case of team sheets, a copy will be provided for the opposing team's administrative purposes for their secure and safe-keeping.

Explicit permission from the DPO must be obtained before removing restricted information, including personal data and confidential information, from WSU premises. Restricted information processed on portable devices and media must be encrypted. A password to an encrypted device must not be stored on the device.

5.4 Third Party Contracts

In the course of its business, WSU may transfer data to third parties to process for a legitimate purpose. Prior to transfer, a contract to ensure compliance with GDPR requirements must be in place with oversight by the DPO, and reviewed on a regular basis. This is to ensure data sharing has an appropriate legal basis and that all third parties will assume liability for any data breach committed by them.

Data handlers / processors for WSU are as follows:

- SAGE – WSU's accounting software
- AEGON – WSU's current pension provider
- NEST – Government pension scheme
- HMRC
- Membership Solutions Limited – in the provision of WSU's website servers
- Advice Pro – advice centre case handling software
- Advice UK - In the provision of case management and customer relationship management
- Cunninghams - ePOS provider
- Survey Monkey Inc. (Survey Monkey and Wufoo)
- University of Worcester

Organisations with whom WSU shares data for legitimate purposes and activities are:

- HMRC
- The Co-operative Bank – WSU's bank
- Knox Cropper Chartered Accountants – WSU's auditors

- Endsleigh Insurance (Brokers) Limited – WSU's insurers – where necessary for processing any claim
- SUSS (Students' Union Superannuation Scheme – closed scheme – where relevant) – WSU's previous pension provider
- University of Worcester
- Tramps Nightclub Limited – WSU sponsor - limited data where agreed
- British Universities & Colleges Sport (BUCS)
- National Governing Bodies
- Volunteering providers – local or national organisations who offer opportunities to our members
- Other Students' Unions and Universities – for sports team sheets
- National Union of Students (for NUS Extra, NUS Media Local, and other limited purposes)
- Charity Commission – regulatory body

6. Policy Monitoring

WSU's management team will monitor compliance with this policy and its procedures through regular reviews and audits. The DPO is responsible for the oversight, revision and updating of this document on a 3-yearly basis or sooner if the needs arises.

7. CCTV

WSU is monitored by the University's CCTV system, to enhance the safety and security of its members, employees and visitors. Details of the University's policy around proper use and purpose of CCTV is available on the University's website.