POLICY – DATA PROTECTION

Owned by: CEO
Date passed: 15/06/23
Body passing: Trustees
Review required: June 2026

1 Policy statement

1.1 Winchester Student Union ("the Union, "we", "us", "our") is committed to the protection of the personal data of students, employees, suppliers and other individuals whom we might hold information about.

1.2 Everyone has rights with regard to how their personal information is handled. During the course of the Union's activities we will collect, store and process personal information and we recognise the need to treat such data in an appropriate and lawful manner.

1.3 The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, customers, students and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards and restrictions on how we may use that information.

1.4 The Union recognises the UK General Data Protection Regulation, tailored by the Data Protection Act 2018 and the Privacy of Electronic Communications Regulations as the primary statutory responsibilities relating to data handling and processing.

1.5 In regard to our staff, this policy does not form part of any employee's contract of employment, and it may be amended at any time. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Union facilities being withdrawn, or even a criminal prosecution. It may also result in personal liability for the individual.

2 Status of the Policy

2.1 This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 The Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. That post is held by Andrew Hodgson, CEO, 01962 82(7429), andrew.hodgson@winchester.ac.uk. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Officer.

2.3 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Data Protection Officer.

3 Responsibilities

3.1 **Students, suppliers and contractors**: Students, suppliers and contractors must ensure that all personal data provided to the Union is accurate and up to date, and that they have read and understood the relevant terms and conditions of engagement with the Student Union. They must ensure that changes of address etc. are updated on the appropriate systems by contacting the relevant staff detailed in the privacy notices at https://www.winchesterstudents.co.uk/privacy-policy

3.2 **Student volunteers:** Committee members, representatives and other student volunteers may handle personal data to administer their activities and services. Students handling such data are required to have completed GDPR training prior to receiving permission to handle any personal data related to their group's or the Union's activities and services. When handling personal data students are required to follow the guidance set out in this policy including the reporting of data breaches, respecting the rights of individuals and secure processing procedures.

3.3 **Union employees:** The Union holds various items of personal data about its employees which are detailed in the Union's UK GDPR Privacy Notice issued to all employees and workers. Employees must ensure that all personal data provided to the Union in the process of employment is accurate and up to date. They must ensure that changes of address etc. are updated by contacting the relevant member of staff within Human Resources.

3.3.1 In the course of day-to-day working it is likely that staff will process individual personal data. Prior to handling any data staff are required to have completed the Union's General Data Protection Regulation training package. In addition to this, staff should maintain a current knowledge of data processing best practice through refresher training and learning available on the Information Commissioner's Office website at www.ico.org.uk. When handling

personal data staff are required to follow the principles of this policy and the privacy notices found at: https://www.winchesterstudents.co.uk/privacy-policy

3.4 **Union managers:** Union managers must ensure that staff handling data in the course of their roles have conducted the appropriate training, are processing data within the frameworks agreed and following the principles of this policy. Managers are also required to conduct annual audits of their relevant spaces, data storage and IT systems to identify weaknesses in information security.

3.5 **Senior Management Team**: The Senior Management Team is required to demonstrate ownership of this Policy and promote it across the Union. The Senior Management Team must gain assurance that these responsibilities are being fulfilled and to ensure resources are available to fulfil the requirements of this policy and associated procedures.

3.6 **The Governing Body**: The Governing Body (Trustee Board) has overall accountability for the strategy of the Union and is responsible for strategic oversight of all matters related to statutory legal compliance and risk for the Union. The Governing Body should seek assurance from the Senior Management Team that effective arrangements are in place to ensure the requirements of this policy.

4 Definition of data protection terms

4.1 **"Data"** is information which is stored electronically, on a computer, or in certain paper-based filing systems. To understand the data the Union collects please see relevant sections of our privacy statement: https://www.winchesterstudents.co.uk/privacy-policy

4.2 **"Data subjects"** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

4.3 **"Personal data"** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

4.4 **"Data controllers"** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish

practices and policies in line with the Act. We are the data controller of all personal data used in the Union.

4.5 **"Data users"** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

4.6 **"Data processors"** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

4.7 **"Processing"** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4.8 **"Sensitive personal data"** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

5 Data protection principles

5.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

5.1.1 Processed fairly and lawfully.
5.1.2 Processed for limited purposes and in an appropriate way.
5.1.3 Adequate, relevant and not excessive for the purpose.
5.1.4 Accurate.
5.1.5 Not kept longer than necessary for the purpose.
5.1.6 Processed in line with data subjects' rights.
5.1.7 Secure.
5.1.8 Not transferred to people or organisations situated in countries without adequate protection.

6 Fair and lawful processing

6.1 The Union will process all data fairly and lawfully and in accordance with GDPR; specifically, that:

6.1.1 The data subject must be told who the data controller is (in this case Winchester Student Union), who the data controller's representative is (in this case the Data Protection Officer), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

6.1.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

7 Processing for limited purposes

7.1 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted. This means that the Union will not collect personal data for one purpose and then use it for another. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose before any processing occurs.

7.2 **Children**: Union staff and volunteers shall not process data related to any individual aged under 13.

8 Adequate, relevant and non-excessive processing

8.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected.

9 Accurate data

9.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

10 Timely processing

10.1 Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, contact the Data Protection Officer.

10.2 Vital records for the purposes of business continuity must be protected from loss, destruction or falsification by Union employees or staff, in accordance with statutory, regulatory, contractual, and Union Policy requirements.

11 Processing in line with data subject's rights

11.1 Data must be processed in line with data subjects' rights. Data subjects have a right to:

11.1.1 Be informed: Know what data is being processed and why

11.1.2 Access: Request access to any data held about them by a data controller.

11.1.3 Rectify: To be entitled to rectify any data if it is inaccurate or incomplete.

11.1.4 Erase: To have data removed where there is no compelling reason for its continued processing.

11.1.5 To restrict: To have data stored but not processed for some uses, eg. opt out of email communications

11.1.6 Data portability: Allowing individuals to obtain and reuse their personal data for their own purposes.

11.1.7 Object: To object to the processing of personal data on the basis of 'legitimate interest'.

12 Data security

12.1 The Union ensures that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

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

12.1.2 Physical representation of data, such as paper forms, must be stored within a locked storage unit. When no longer needed, the e-copies should be deleted and any paper copies securely destroyed.

12.2 Personal data will only be transferred to a third-party data processor if they agree to comply with Union procedures and policies, or if they put in place adequate measures themselves.

12.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

12.3.1 **"Confidentiality"** means that only people who are authorised to use the data can access it.

12.3.2 **"Integrity"** means that personal data should be accurate and suitable for the purpose for which it is processed.

12.3.3 **"Availability"** means that authorised users should be able to access the data if they need it for authorised purposes.

12.4 Security procedures include:

12.4.1 **"Entry controls."** Any stranger seen in entry-controlled areas should be reported.

12.4.2 **"Secure lockable desks and cupboards."** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

12.4.3 **"Methods of disposal."** Paper documents should be shredded or disposed of via the confidential waste receptacle. flash drives should be fully reformatted when they are no longer required.

12.4.4 **"Equipment."** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from or lock securely, their PC when it is left unattended.

13 Dealing with subject access requests

A formal request from a data subject for information that we hold about them must be made in writing (including email). Any Union officer or staff member who receives a written request should forward it to the Data Protection Officer immediately.

14 Providing information over the telephone

14.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

14.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.

14.1.2 Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

14.1.3 Refer to their line manager **or** the Data Protection Officer for assistance in difficult situations.

15 Monitoring and review of the policy

15.1 Compliance with the procedures laid down in this policy will be monitored via the Union's Senior Management Team, together with reviews by the Trustee Board.

15.2 The Data Protection Officer is responsible for the monitoring, revision and updating of this document on a 3 yearly basis, or sooner if the need arises.