



## Data Protection Policy

### 1 Scope and Purpose

- 1.1 This policy is written with due regard to the principles and guidelines laid out in the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR); UK Data Protection Bill (when enforced) (the “data protection legislation”) and other guidance available from relevant professional or regulatory bodies, such as the Information Commissioner. Data protection legislation controls how personal information is used by organisations, businesses or the government. Everyone responsible for using personal data has to follow strict rules called ‘data protection principles
- 1.2 This policy works in conjunction with the Students’ Union Privacy Policy, Email Etiquette Policy, and the University Data Protection Policy, and Acceptable Use Policy for IT Facilities and Equipment and applies to records about individuals who can be identified from that data – personal data.
- 1.3 The purpose of this Policy is to ensure that the Students’ Union and its staff (both permanent and student), comply with the data protection laws when processing (obtaining, holding, using, disclosing, disposing etc.) personal data.
- 1.4 Personal data is defined as:  
  
*any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’ (GDPR Article 4(1))*
- 1.5 Personal data that reveals an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health, and individual’s sex life or sexual orientation is classed as “special categories of personal data” and merit specific additional protection.
- 1.6 This Policy applies to all personal data processed by the Students’ Union, regardless of whether that data is held on Students’ Union or University equipment or personally owned equipment used inside or outside Students’ Union premises.
- 1.7 In law the Students’ Union is a “Controller” required to ensure all personal data it is responsible for is processed in accordance with the data protection legislation. The Controller is also required to ensure anybody acting under their authority i.e. staff and contractors, who has access to the Students’ Union’s personal data only processes that data in accordance with the controller’s instructions, which are:-

#### 1.8 Personal data shall be:

- Processed lawfully and fairly and in a transparent manner in relation to the data subject;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures; and
- The controller shall be responsible for and able to demonstrate compliance with these principles (GDPR Article 5 Paras 1&2)

## 2 Responsibilities

2.1 The Students' Union is the Controller and legally responsible for establishing appropriate technical and organisational measures to ensure compliance with data protection legislation.

2.2 When acting as a Processor (processing personal data on behalf of another controller under contract), the Students' Union is (a) responsible for acting only in accordance with the Controller's documented instructions and (b) ensuring the protection of that personal data through effective organisational and technical measures.

## 3 Governance

3.1 The Students' Union Chief Executive is the Data Protection Officer (DPO) and is responsible for:

- Informing and advising the Trustee Board and everybody involved in the processing of personal data of their obligations pursuant to the data protection legislation;
- Promoting and monitoring compliance with the legislation, including raising awareness and training; producing policy and guidance; providing advice and managing risks.
- Ensuring data protection impact assessments are completed appropriately, providing advice and monitoring its performance pursuant to GDPR Article 35;
- Ensuring compliance with subject access rights and ensuring that data is disclosed in accordance with subject access legislation pursuant to GDPR Article 15;
- Ensuring data protection breaches are documented, reported, investigated and resolved and when appropriate reported to the Information Commissioner's Office pursuant to GDPR Article 33;
- Cooperating with the Information Commissioner's Office (the supervisory authority); and
- Acting as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.

3.2 The DPO is also responsible for ensuring the Students' Union's Data Protection Notification is registered with the Information Commissioner's Office and for reviewing this Policy in line with current legislation, codes of practice and regulatory standards.

#### **4 Staff responsibilities**

4.1 Access to personal data is only provided to authorised staff who need it to be able to perform their essential contracted duties.

4.2 Staff members processing personal data about YSJU students, other staff, or any other identifiable individual must comply with this policy. This includes any voluntary, short-term or contracted staff.

4.3 In particular staff members must ensure that they:

- Comply with the data protection principles when obtaining, using, disclosing or otherwise processing personal data.
- Keep all personal data securely in accordance with this Policy and the University Acceptable Use Policy for IT Facilities and Equipment and related guidance;
- Only disclose personal data to persons authorised to receive it when it is appropriate to do so;
- Do not disclose personal data accidentally or otherwise, to any unauthorised person/third party (staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Chief Executive;
- Maintain and dispose of personal data in accordance with the Students' Union's Records Management Policy and retention schedules;
- Direct any queries regarding data protection, including subject access requests and complaints, to the Chief Executive;
- Report any data protection breaches to the Chief Executive and provide support to ensure the incident is appropriately investigated and resolved.
- Seek advice from the Chief Executive about data protection matters when in doubt;
- Ensure student groups they work with are aware of their responsibilities for data protection.

#### **5 Processors**

5.1 A "processor" is somebody other than Students' Union staff who processes personal data on behalf of the Students' Union – usually an external company working under contract.

5.2 When a processor is used, the Students' Union as Controller retains responsibility and liability for the secure and lawful processing of the personal data being processed. The controller can only appoint a processor:

- who can provide sufficient guarantees about its technical and organisational security measures to protect personal data and meet the requirements of the GDPR;
- processes personal data only in accordance with the instructions of the controller set out in a written contract;
- does not appoint a sub-contractor without the written permission of the controller.

## **6 Students and recognised Student Groups**

6.1 Students and recognised Student Groups, such as Sports Teams and Societies, are responsible for ensuring compliance with this policy when processing personal data under the jurisdiction of the Students' Union and in particular when conducting activities involving individuals that includes the collection and use of participants' personal data.

## **7 Lawful basis for processing**

7.1 Any processing of personal data must be done in compliance with the data protection legislation and in particular will only be lawful if one of the conditions is Article 6 – Lawfulness of processing applies; and, where special categories of personal data are used both a condition in Article 6 and a condition in Article 9 must apply.

7.2 Where Article 6 Section 1(f) condition - processing is necessary for the purpose of the legitimate interests (of the Students' Union and/or University) applies, a Legitimate Interests Assessment (LIA) must be completed to justify the Students' Union and/or University's legitimate interests do not override the individual data subject's fundamental rights and freedoms.

## **8 Rights of the data subject**

8.1 The Students' Union respects the fundamental rights and freedoms of data subjects and will uphold their rights by ensuring:

- Concise, transparent, intelligible and easily accessible information is provided to explain the reasons why the Students' Union collects and uses personal data and the lawful basis for this;
- Subject access requests are responded to fully in accordance with GDPR Article 15 (subject to verification of identity and right to access);
- Rights concerning rectification, erasure, restrictions, portability and erasure of personal data are upheld (unless the Students' Union cannot comply for legal reasons and is required to apply an exemption)
- The individual data subject's legitimate right to object to the processing of their personal data for certain purposes is respected;
- Consent is obtained when it is required to provide the lawful basis for processing personal data;
- Personal data is protected by technical and organisational controls at all times.

## **9 Information Security**

9.1 Technical and organisational measures shall be implemented to ensure personal data is protected against risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed which may lead to physical, material or non-material damage.

9.2 As the majority of IT equipment used by the Students' Union is that of YSJU, the University's Acceptable Use Policy for IT Facilities and Equipment and guidelines shall be followed to ensure the protection of:

- Confidentiality - ensuring that personal data is only accessible to authorised users;

- Integrity - safeguarding the accuracy and completeness of personal data;
- Availability - ensuring that authorised users have access to information and systems when and where required.

## 10 Personal Data Security Breach Incidents

- 10.1 A personal data security breach is any incident that involves a failure of the Students' Union and/or University's technical and organisational measures resulting in any unauthorised or unlawful processing, accidental loss, destruction of or damage to personal data.
- 10.2 The GDPR introduces a new duty on all organisations to report certain types of personal data breaches to the Information Commissioner's Office within 72 hours of becoming aware of the breach. In certain circumstances individuals whose personal data has been compromised by the breach must also be notified.
- 10.3 The Chief Executive must be informed of a data security breach incident as soon as it becomes known and their advice should be followed without delay.

## 11 Privacy by Design

- 11.1 The GDPR introduces a new requirement for organisations to carry out a data protection impact assessment (DPIA) prior to embarking on a project that has an impact on the way personal data is processed e.g. the implementation of a new IT system for collecting, storing and accessing personal data; a new data sharing initiative etc. A DPIA enables the organisation to identify and mitigate the associated privacy risks and ensure data protection compliance is built into the design, including being able to demonstrate compliance with legal obligations.
- 11.2 In such a case the Students' Union adopts the University's Data Protection Impact Assessment Procedure, which should be followed when:
  - Developing a new IT system for storing and accessing personal data.
  - Negotiating a new data sharing initiative where two or more organisations seek to pool or link sets of personal data.
  - Designing a proposal to identify people in a particular group or demographic and initiate a course of action e.g. profiling or research.
  - Planning to use existing data for a new and unexpected or more intrusive purpose
  - Introducing new policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.
- 11.3 The University's DPO is responsible for providing advice, ensuring the process is completed appropriately and monitoring its performance pursuant to GDPR Article 35.

## 12 Information Asset Register

- 12.1 GDPR Article 30 imposes a new requirement on a controller to maintain a record of processing activities under its responsibility, and specifies what information that record should contain.

- 12.2 The Students' Union has an Information Asset Register for this purpose. This is held and maintained by the Chief Executive and all staff are reminded to ensure the Chief Executive is informed if there are any additions necessary for the register.

### **13 Guidance**

- 13.1 The Information Commissioner's Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements