**Data Protection Policy**

**Context and overview**

**Introduction**

This Data Protection Policy describes how personal data must be collected, handled and stored to meet the University of Stirling Students’ Union’s data protection standards – and to comply with General Data Protection Regulation (GDPR).

The University of Stirling Students’ Union needs to gather and use certain information about individuals. These can include student members, employees, volunteers or individuals within partners who supply us with goods or services and other people the organisation has a relationship with or may need to contact.

The University of Stirling Students’ Union is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data. This policy describes how this personal data must be collected handled and stored to meet the organisation’s data protection standards and comply with GDPR.

This policy and processes established in managing our data compliance has had oversight and guidance from their HR /Legal specialists and the Students’ Union Trustee Board

**Why this policy exists**

This data protection policy ensures the University of Stirling Students’ Union:

* Complies with GDPR and protects the rights of student members, employees, volunteers and individuals or individuals within partners who supply us with goods or services
* Is open about how it stores and processes individuals’ data
* Protects itself from the risks of data breach

**General Data Protection Regulations (GDPR)**

We comply with GDPR legislation and will undertake to do the following;

Only process as much personal data as is necessary for our administration and the services we supply.

Only hold such data for so long as necessary for those purposes. In this connection we have decided that ten years following the last contact with an individual is usually an appropriate period to hold data covering the legal limitation period (six years) and a moderate margin. As in most cases this is only archived data, not sensitive, not dangerous and will not be used if there seems little risk to data subjects.

Only process such data on grounds for lawful processing provided within GDPR Article 6.

Not engage in direct marketing to student members or suppliers otherwise than in accordance with the relevant legislation and guidance from the ICO.

Utilise appropriate organisational and technical measures to ensure that Personal Data processed by us is kept secure.

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.

Not transfer Personal Data (which includes giving third parties access to it within our IT system) to recipients located outside the European Economic Area and the UK without confirmation that such transfer is lawful.

Update this document from time to time so that it remains an accurate record of our data processing activities and policies.

**People, risks and responsibilities**

**Policy scope**

The University of Stirling Students’ Union needs to gather and use information about individuals. These can include student members, employees, volunteers and individuals or individuals within partners and any other people the organisation has a relationship with or may need to contact.

Protecting the confidentiality and integrity of personal / sensitivedata is acritical responsibility that the University of Stirling Students’ Union takes seriously at all times.

**Key Definitions**

**Data Processing**

The definition of ‘data processing’ includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

**Personal Data**

‘Personal data’ is information about a living individual, who is identifiable from that information or who could be identified from that information combined with other data which the University either holds or is likely to obtain. This includes names, contact details, photographs, salary, memberships in clubs and societies, sickness absence, leave, dates of birth, marital status, personal email address, etc. Furthermore, any expression of opinion or any intentions regarding a person are also considered ‘personal data’.

Examples which would not normally be classed as personal data include: attendance at meetings or mention in minutes, unless the meeting is about the named individual; University email address and telephone number, or names on emails/letters/memos unless the body of the document is about the named individual.

**Sensitive Personal Data**

Sensitive personal data is a special category of information which relates to a data subject’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. It also includes personal data relating to criminal offences and convictions.

Where employees or students have disclosed a disability or other sensitive personal data, this information will be shared on a strictly need to know basis.

This policy applies to:

* The University of Stirling Students’ Union
* All student members, employees, volunteers and individuals or individuals within partners University of Stirling Students’ Union

It applies to all data that the University of Stirling Students’ Union holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

* Names of individuals
* Postal addresses
* Email addresses
* Telephone numbers
* Student numbers
* …plus any other information relating to individuals

**Data protection risks**

This policy helps to protect University of Stirling Students’ Union from some very real data security risks, including:

* **Breaches of confidentiality.** For instance, information being given out inappropriately.
* **Inappropriate use of data.** For instance, ensuring that information provided is only used for the legitimate purposes of the Union.
* **Reputational damage.** For instance, the University of Stirling Students’ Union could suffer if hackers successfully gained access to sensitive data.

**Responsibilities**

Everyone who works for or with University of Stirling Students’ Union has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

* The **Trustee Board** is ultimately responsible for ensuring that University of Stirling Students’ Union meets its legal obligations.
* The **Data Controller – Chief Executive,** is responsible for:
  + Keeping the board updated about data protection responsibilities, risks and issues.
  + Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  + Arranging data protection training and advice for the people covered by this policy.
  + Handling data protection questions from staff and anyone else covered by this policy.
  + Dealing with requests from individuals to see the data University of Stirling Students’ Union holds about them (also called ‘subject access requests’).
  + Checking and approving any contracts or data sharing agreements with third parties that may handle the University of Stirling Students’ Union’s sensitive data.
* The Communications **Manager,** is responsible for:
  + Approving any data protection statements attached to communications such as emails and letters.
  + Addressing any data protection queries from journalists or media outlets like newspapers.
  + Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

**General staff guidelines**

* The only people able to access data covered by this policy should be those who **need it for their work.**
* Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
* **University of Stirling Students’ Union will provide training** to all employees to help them understand their responsibilities when handling data.
* Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
* In particular, **strong passwords must be used** and they should never be shared.
* Personal data **should not be disclosed** to unauthorised people, either within the University of Stirling Students’ Union or externally.
* Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of. See data retention guide appended to this policy
* Employees **should request help** from their line manager or the data controller if they are unsure about any aspect of data protection.

**Data storage**

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data controller.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

* When not required. The paper or files should be kept **in a locked drawer or filing cabinet** the University of Stirling Students’ Union operates a **clear desk policy**
* Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
* **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

* Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
* If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
* Data should only be stored on **designated drives and servers,** and should only be uploaded to an **approved cloud computing services.**
* Servers containing personal data should be **sited in a secure location,** away from general office space.
* Data should be **backed up frequently**. Those backups should be tested regularly, in line with the University of Stirling Students’ Union’s standard backup procedures.
* Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
* All servers and computers containing data should be protected by **approved security software and a firewall.**

**Data use**

Personal data is of no value to University of Stirling Students’ Union unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk corruption or theft:

* When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
* Personal sensitive data **should not be shared informally.** In particular, it should never be sent by email, as this form of communication is not secure.
* Personal sensitive data must be **encrypted before being transferred electronically**.
* Personal data should **never be transferred outside of European Economic Area.**
* Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

**Data accuracy**

The law requires University of Stirling Students’ Union to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater effort the University of Stirling Students’ Union should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

* Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
* Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a student/customer’s details when they call.
* University of Stirling Students’ Union will make it **easy for data subjects to update the Information** University of Stirling Students’ Union holds about them. For instance, via the University of Stirling Students’ Union website.
* Data should be **updated as inaccuracies are discovered.** For instance, if a member/customer can no longer be reached on their stored telephone number, it should be removed from the database.
* It is the communications manager’s responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

**Subject access requests**

All individuals who are the subject of personal data held by University of Stirling Students’ Union are entitled to:

* Ask **what information** the University of Stirling Students’ Union holds about them and why.
* Ask **how to gain access** to it.
* Be informed **how to keep it up to date**.
* Be informed how the University of Stirling Students’ Union is **meeting its data protection obligations.**

If an individual contacts the University of Stirling Students’ Union requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at [theunion@stir.ac.uk](mailto:theunion@stir.ac.uk) . The data controller can supply a standard request form, although individuals to not have to use this.

The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

**Disclosing data for other reasons**

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, University of Stirling Students’ Union will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the University of Stirling Students’ Union’s legal advisers where necessary.

**Privacy Notices**

University of Stirling Students’ Union aims to ensure that individuals are aware that their data is being processed, and that they understand:

* How the data is being used
* How to exercise their rights

To these ends, the University of Stirling Students’ Union has a privacy notices, setting out how data relating to individuals is used by the University of Stirling Students’ Union.

(This is available on request. A version of this statement is also available on the University of Stirling Students’ Union’s website).

**Link to privacy notices policy**

**Further Information**

Further detailed information regarding data protection is available within the staff handbook;

Employee Data Policy

Recruitment Policy

Computers, Internet and Email Policy