Data Protection Policy

Approved June 18

Document Author(s):	Louise Dixon / Donna Thompson
Relevant to:	All staff
Responsibility for Policy:	Chief Executive and Trustees
Responsibility for document review:	Data Protection Coordinator / Chief Exec
Document introduced:	May 2018
Next Review Date:	May 2020

**The Data Protection Coordinator reserves the right to amend this document at any time should the need arise.*

Introduction

Sunderland Students Union ('Sunderland SU') is fully committed to compliance with the requirements of the General Data Protection Regulation ('GDPR'); which from 25 May 2018 replaces the Data Protection Act of 1998. Sunderland SU recognises in full the rights and obligations established by this data protection law in relation to the management and processing of personal data.

This policy is intended to serve as general guidance for staff and students in implementing the letter and spirit of the provisions and principles of the GDPR.

The Union will therefore follow procedures which aim to ensure that all members, elected officers, employees, contractors, agents, consultants, or other partners of the Union who have access to any personal data held by or on behalf of the Union, are fully aware of and abide by their duties under the GDPR. The Nominated Person(s) Central Services Manager (Data Protection Coordinator) has responsibility for the Data Protection Policy.

Data Protection Advice

The Nominated Person(s) the Central Services Manager is the Data Protection Coordinator for Sunderland SU and provides general advice on data protection.

The Data Protection Coordinator should be informed of all data subject access requests received by Sunderland SU staff (see page 10 for further details).

Guidelines and good practice notes on compliance with data protection law can be found on Sunderland SU's website at www.sunderlandsu.co.uk/dataprotection

Advice on specific issues concerning the handling of personal data may also be contained within the relevant policy.

Why is Data Protection Important?

The GDPR requires organisations, including Sunderland SU, to ensure that the information they hold on individuals is stored appropriately. Under the GDPR Sunderland SU is categorised as a Data Controller in respect of much of this information.

The purpose of the GDPR is to protect the rights and privacy of individuals, and to ensure that data about them is not processed without their knowledge and is processed with their consent wherever possible.

All staff must be aware of the need to handle personal data in line with the GDPR and on commencement of employment, compulsory online training must be completed https://www.usonline.co.uk/news/gdpr-and-you. Once completed this

must be logged with the Central Services Manager for retention on their personnel file.

Statement of Policy

In order to operate efficiently, Sunderland SU has to collect and use information about people with whom it works. These may include members of the Union, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

This personal information must be handled and dealt with properly however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the GDPR to ensure this.

The Union regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between itself and those with whom it carries out business. The Union will ensure that it treats personal information lawfully and correctly. To this end the Union fully endorses and adheres to the principles of data protection as set out in the GDPR.

The Principals of Data Protection

Data protection law stipulates that anyone processing personal data must comply with **Six Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information shall:

- Be processed fairly and lawfully and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency');**
- Be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes **('purpose limitation');**
- Be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which it is processed **('data minimisation');**
- Be accurate and where necessary, kept up to date with every reasonable step taken to ensure that inaccurate personal data is erased or rectified without delay **('accuracy');**
- Be kept in a form which permits identification of the data subject for no longer than is necessary, and for the purpose of which the personal data is processed **('storage limitation');**

- Be kept secure i.e. protected by an appropriate degree of security against unauthorised or unlawful processing and against accidental loss, destruction or damage **('integrity and confidentiality').**

In addition, the GDPR:

- requires proof of compliance with the 6 principles above **('accountability');**
- restricts personal data being transferred to outside of the European Economic Area, unless that country or organisation ensures an adequate level of data protection;
- provides conditions for the processing of any personal data **('processing conditions');** and
- makes a distinction between personal data and **"special category"** personal data.

Definitions

Personal Data

means any information relating to an identified or identifiable living person **('data subject');** an identifiable natural person is one who can be identified, directly or indirectly, such as by reference to an identifier e.g. 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.

Data Controller

A person or organisation (including public authority, agency or other body) which, alone or jointly with others, determines the purposes for which and the manner in which any personal data, are, or are to be, processed.

Data Processor

Any person or body (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Subject

A living individual who is the subject of the personal data.

Processing

Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

organising, structuring, storing, adaptation or alternating, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special category personal data is 'Personal Data' which reveals an individual's health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic /biometric data (such as finger prints) or sexual orientation/sex life.

Third Party

Any person other than a data subject or the data controller or any data processor or other person authorised to process data for the data controller or processor.

Handling of Personal/Sensitive Information

Sunderland Students Union will, through appropriate management and the use of strict criteria and controls;

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under data protection law; these include:
    - The right to be informed that processing is being undertaken;
    - The right of access to one's personal information within 1month, unless an exception applies;
    - The right to prevent processing in certain circumstances;

- The right to request correction, rectification, prevention from processing or erasure of personal information;
- The right to object to marketing; and
- The right to data portability (allowing individuals to obtain and reuse their personal data for their own purposes across different services).

In addition, the Union will ensure that:

- There is someone with specific responsibility for data protection The Nominated Person(s) 'Central Services Manager' in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are dealt with promptly and courteously;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

Responsibilities of Officers, Staff and Other Parties

All elected officers are to be made fully aware of this policy and of their duties and responsibilities under the GDPR.

- All managers and staff within the Union will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:
- Paper files and other records or documents containing personal/special category data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of robust authentication mechanisms to prevent unauthorised access to University data, and secure passwords, which have forced changes periodically. Access to any given file or data has to be granted by the data owner, system owner or owner of the Filestore, SharePoint site or database.
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other agents of the Union must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Union, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the GDPR. Any breach of any provision of the GDPR will be deemed as being a breach of any contract between the Union and that individual, company, partner or firm;
- Allow data protection audits by the Union of data held on its behalf (if requested);
- Indemnify the Union against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.
- All contractors who are users of personal information supplied by the Union will be required to confirm that they will abide by the requirements of the GDPR with regard to information supplied by the Union.

The Information Sunderland SU holds

Sunderland SU holds a wide range of information on individuals. This information is managed, on a day-to-day basis for four main areas:

- Policy, Campaigns & Communications (Policy & Campaigns, Representation, Marketing & Communications/Digital Media & Design)
- Members Support (Information, Advice & Guidance, Wellbeing, Activities and Opportunities)
- Central Services (Central Services, Admin Assistant, Drivers)

- Finance

As each area requires information for a different purpose, methods of collection and storage vary.

Each area, therefore must liaise with the Central Services Department on an annual basis to update the GDPR compliance register in relation to the data that they collect and process.

Processing Conditions

In order for personal data to be processed, at least one of the following processing conditions must exist:

- the data subject has given consent to the processing of their personal data (there is a high threshold for valid consent; therefore it should only be relied upon in limited circumstances. Furthermore, individuals have the right to withdraw the consent that they give at any time);
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Sunderland SU have legitimate interests;
- compliance with a legal obligation; or
- processing is required to protect the vital interests of the data subject or of another individual; or for the establishment, exercise or defense of legal claims.

Records of the processing conditions relied upon must be maintained in all circumstances. In particular, where consent is relied upon, records of the actual consent obtained should be maintained.

Privacy Notices

Personal data must be processed fairly. The most usual method of achieving this is by ensuring that the data subject has access to a data protection statement, (known as a Privacy Notice) included on all forms capturing personal data, within guidance notes for the completion of forms, in relevant staff and student handbooks, and on any forms completed online.

Guidance on data privacy notices is available in the Guidance Notes and Statements on our website www.sunderlandsu.co.uk/dataprotection

Implementation

The Nominated Person(s) Central Services Manager is responsible for ensuring that the Policy is implemented and will have overall responsibility for:

- The provision of cascade data protection training, for staff within the Union.
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence, throughout the Union, with the GDPR.

Accountability

Sunderland SU is responsible for and must be able to demonstrate compliance with the GDPR. Documentation evidencing compliance with the GDPR will need to be produced to the Information Commissioner on request.

In particular, there are obligations throughout the GDPR which require documentation to be kept, this includes the obligation to maintain records of all processing activities which specify details such as data retention periods, extra EEA transfers of personal data, evidence of consent and the recipients of personal data.

To this end, SLT will be responsible for ensuring the maintaining of records, reporting and updating the Nominated Person(s) Central Services Manager (Data Protection Coordinator) of the processing of personal data, within their department/area.

The Nominated Person(s) Central Services Manager (Data Protection Coordinator) will review the Sunderland SU Data Register with the relevant departments annually, prior to notification to the Information Commissioner and conduct 3 monthly spot checks of all departments.

To this end, any changes made between reviews will be brought to the attention of the Nominated Person(s) Central Services Manager (Data Protection Coordinator) immediately.

Right of Subject Access

The GDPR gives data subjects the right to know whether their personal data is being processed by Sunderland SU and, if so, to access their personal data.

The Nominated Person the Data Protection Coordinator should be informed of all 'data subject access requests' received by Sunderland SU staff.

A valid data subject access request must be made in writing (and this includes e-mail requests).

The individual should be told by Sunderland SU within 1 calendar month of receipt of the request whether Sunderland SU are processing the individual's personal data and if so:

- the purposes for which the data is being processed;
- to whom the data is or may be being disclosed to;
- the period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from Sunderland SU the rectification or erasure of the personal data or restriction of processing of personal data concerning the individual or to object to such processing;
- the right to lodge a complaint with the information commissioner; and
- where the personal data is transferred to a third country or to an international organisation, the data subject's right to be informed of the appropriate safeguards in place;
- to receive in an intelligible manner, a copy of their personal data.

Sunderland SU may, only in very limited circumstances, such as those involving excessive requests, ask for payment of a fee.

Sunderland SU must ensure that it has proof of the identity of the requestor to prevent an unlawful disclosure.

A data subject can request access to their personal data through another party such as a lawyer or an advocate. A signed letter or form of authority from the data subject must be provided before any data is disclosed.

Whilst Sunderland SU is required by the GDPR to respond within 1 calendar month of receipt of the request, every effort should be made to respond as quickly as possible. The deadline applies to all requests for personal data, whether routine or complex.

If the request arises as part of another matter for instance a complaint, grievance or disciplinary matter, the requirements of the GDPR must not be overlooked, particularly the 1 month deadline. In these circumstances, staff must seek advice from the Nominated Person(s) Data Protection Coordinator.

The requested data should normally be provided in the format the request was received unless the data subject requests otherwise.

Sunderland SU has a guidance note on data subject access requests, which can be found within the following section of our website at: www.sunderlandsu.co.uk/dataprotection

If the data subject believes that their personal data is inaccurate, out-of-date, held unnecessarily or is offensive, they have the right to have the information rectified, blocked, erased or destroyed. The data subject also has the right to insist that Sunderland SU ceases to process their personal data if such processing is causing or is likely to cause unwarranted substantial damage or substantial stress to them or to another. The data subject may also have a right to compensation if it can be proven that damage or distress has been caused.

Guidance on the right to prevent the processing of personal data can be found at:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/

Third Party Data Rights

When handling a subject access request, sometimes another individual (known as a third party) may be identified in the personal data to be disclosed. Sunderland SU will only disclose third party data under the GDPR where it does not adversely affect the rights and freedoms of the third party. Guidance can be obtained from the Nominated Person(s) Data Protection Coordinator

Exemptions

There are number of exemptions from the provisions of the GDPR. These allow Sunderland SU to either disclose or withhold data from disclosure in particular circumstances, without breaching the data protection principles. Guidance on the exemptions and their application can be obtained from the Nominated Person(s) Data Protection Coordinator.

General Responsibilities of Sunderland SU Staff

When processing personal data, Sunderland SU staff must ensure that they abide by the GDPR, and process data in accordance with the eight data protection principles.

If in any doubt, staff should refer to this policy, any other guidance provided on our website or the Nominated Person(s) Data Protection Coordinator.

Security of Data

Sunderland SU staff responsible for processing personal data must ensure that it is kept securely to avoid unauthorised access and only disclose to those authorised to receive it.

Sunderland SU has policies and procedures in regard to the security of electronically held data and staff must ensure that they read and understand these policies and procedures.

All staff and students are required when they first log onto the University's network to confirm their understanding and acceptance of the University's IT Systems Terms and Conditions of Use as detailed in the University's IT acceptable use policy which is publicly located at: www.sunderland.ac.uk/aup

Care must be taken to ensure that PCs and terminals on which personal data is viewed are not visible to unauthorised persons, especially in public places. Screens showing personal data should not be left unattended. Staff should use the facility "lock computer" on their PC if they are absent from their desk for a short period of time, and should "log-off" for longer periods.

In the case of manual data, files containing personal data should be kept in locked storage cabinets when not in use. Procedures for booking files in and out should be used so that their movements can be tracked. Files should not be left on desks overnight.

Sunderland SU provides facilities for the confidential destruction of paper documents. Details of this service and related guidance are available on our website: www.sunderlandsu.co.uk/dataprotection

External Legal Advice

Sunderland SU staff should not seek external legal advice directly from the Union's lawyers or data protection advice from any other source, without consulting first with the Nominated Person(s) Data Protection Coordinator.

The Role of the Information Commissioner

The Information Commissioner is an independent official appointed by the Government to oversee the GDPR, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. The Commissioner reports annually to Parliament. The Commissioner's decisions are subject to the supervision of the Courts and the Information Tribunal.

The mission of the Office of the Information Commissioner is to promote public access to official information and to protect personal information.

The Information Commissioner provides good practice guidance and interpretation of the GDPR for data controllers and advice to the public on how to access personal data. The website of the Office of the Information Commissioner is: https://ico.org.uk/

The Commissioner has formal powers to force a data controller to take or refrain from certain actions if the Commissioner has determined there has been or is likely to be a breach of the GDPR. Failure to comply with a Decision or an Enforcement Notice may be dealt with as though Sunderland SU had committed contempt of court. As from 25 May 2018, the Information Commissioner (ICO) is able to impose fines of up to **20,000,000** euros (or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher) as a penalty for serious breaches of the GDPR.

Breach Management at Sunderland SU

Guidance for Records Management staff setting out the procedures to follow once a GDPR breach has been identified:

Why should I follow this guidance?

Breaches of the GDPR have become an increasingly high profile issue. A breach could damage Sunderland SU's reputation and its relationship with its stakeholders or expose the University, its staff or students to risks including fraud, identity theft and distress. Sunderland SU could be sued or fined up to 20,000,000 euros or up to 4 % of the total worldwide annual turnover.

What should I do when a breach occurs?

A breach means any breach of security leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

If a breach occurs, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

The Nominated Person the Central Services Manager (Data Protection Coordinator) will deal with the breach. In her absence it will be dealt with by the most senior member of staff available at the time.

Please see below for a step by step guide to the procedures that staff must follow when they are made aware of a breach:-

On discovery of a breach

Once you have confirmed that a breach has occurred, collect details of the exact nature of the breach and inform the Chief Executive immediately.

Contact the relevant area

Contact the freedom of information practitioner of the area concerned immediately. Ensure that you explain: the exact nature of the breach

- an indication of the seriousness of the breach
- what the area needs to do to stop being in breach of the GDPR
- the fact that this matter needs to be dealt with as a matter of urgency
- Contact the head of the department responsible for the information affected by the breach.

Monitor the situation closely to ensure that the department responsible for the breach remedies the breach as soon as possible.

Preventing a repetition of the breach

Investigate how the breach occurred and make sure that process and procedures are amended to ensure that this type of breach does not happen again.

Managing the consequences of the Breach

Inform the Nominated Person(s) Data Protection Coordinator as quickly as possible.

With guidance from the Nominated Person(s) Data Protection Coordinator, consider whether the breach is sufficiently serious that the Information Commissioner needs to be informed. If so, the GDPR requires that the Information Commissioner is notified no later than 72 hours after becoming aware of the personal data breach.

When you inform the Nominated Person(s) Data Protection Coordinator, you should try to identify whether the breach is serious, such as where:

- there is the potential for journalistic involvement (for example is it possible that a member of the public may find the data and pass it to a journalist?);
- special category personal data is involved in the breach;
- the breach involves a large volume of data or affects a lot of people;

With guidance from the Nominated Person(s) Data Protection Coordinator, it may be necessary to contact all the data subjects affected by the breach. If so we must explain the situation and detail the steps we are taking to protect their personal details. This can be done either individually or, if a large number of people are affected, it may be appropriate to publish details on our website.

Breaches and Sunderland SU's Disciplinary Policy

Any data breaches by staff will be careful investigated and dealt with through the Union's disciplinary policy and considered as gross misconduct given the level of importance.

Data Protection at USSU

For further information, the Nominated Person(s) Data Protection Coordinator at Sunderland SU is the Central Services Manager and full details of the University's Data Protection Policy and supporting documents can be found at: www.sunderlandsu.co.uk/dataprotection

How to make a Subject Access Request

This section is intended to assist you in making a Subject access Request under the GDPR. It is not intended to serve as a comprehensive guide or instruction, and we would recommend that you also visit the Information Commissioner's office website which provides further information and guidance on making a Subject Access Request.

Before making a Subject access Request, you should think about what it is you want to know and whether a formal request is necessary. If may be possible to make an informal request, for example a routine enquiry about whether we have received payment of your tuition fees. If we can answer your request quickly as a routine matter, this will save you the time of going through the Subject Access Request process. If it is not possible for us to handle your request informally, for example, if you would like to see a full record of your student record we will tell you that is the case and you will need to make a formal request.

1.1 How to make your Subject Access Request

Subject access requests must be made in writing, and should include the following information. This will help us identify you, and understand the nature of your request:

- Full name
- Address
- Telephone number
- Email address (if you would like us to communicate with you by email)
- Identity information, such as a copy of your driving licence, your student ID or employee number and faculty in which you are a student or staff member, which will help us to identify you particularly where we have personal data relating to individuals with the same name
- The specific right that you wish to exercise, including full details of the information that you require and any relevant dates

You can either male a Subject Access Request by completing and returning our subject access form by email to centralservices@sunderland.ac.uk or you can write to the address below:

Central Services
Students' Union
Ground Floor, Edinburgh Building
Chester Road, City Campus
Sunderland, SR1 3SD

You should always keep a copy of your request for future reference.

We cannot release personal data to anybody other than the data subject unless we have their express consent to do so. Therefore, where a Subject Access Request is made on behalf of the data subject, the request must also include proof that the data subject has consented to the request and to their personal data being provided to that person.

1.2 When will you receive a response to your Subject Access Request?

Following receipt of your request we will have 30 days in which to respond to Subject access Requests made under the GDPR. We will be able to extend the period of compliance by a further two months where requests are more complex or numerous. If this is the case we will inform you within one month of the receipt of the request and explain why the extension is necessary. This timeframe runs from the date when we receive your request and any additional information that we ask you to provide to enable us to identify you. We will write to you to confirm we have received your request and request any information that we require in order to identify you. We may charge a reasonable fee when a request is manifestly unfounded or excessive particularly if it is repetitive.

1.3 How will we respond to your Subject access Request?

Once we have been able to identify you, we will conduct searches of our records to identify what personal data we hold about you in order to respond to your subject access Request within the above timeframe.

Our response will either provide you with the information you have requested, or inform you that we do not hold that information.

Where you have asked us to provide you with a copy of personal information held, we will provide you with a copy sent in the same manner as your request, unless you request otherwise. For example, if you original Subject access Request is made in writing by post, we will respond to you and provide you with a hard copy of the personal data by recorded post unless you ask us to send it to you by email or other means.

1.4 Can Sunderland Students' Union Group withhold information?

The GDPR allows us to withhold certain information when responding to your Subject Access Request if disclosing the information would adversely affect the rights and freedoms of others. This includes information about other people which

may be recorded together with your personal data. We are not permitted to share anybody else's information without their consent.

1.5 What to do if you are unhappy with our response

If you are unhappy with our response, for example if you believe you have not received all of the information that you requested, please write to us at Central Services, Students' Union, Ground Floor, Edinburgh Building, Chester road, City Campus, Sunderland, SR1 3SD or you can email centralservices@sunderland.ac.uk and set out your concerns In as much detail as possible. For example, if you think that the information sent to you is incomplete, please tell us what it is you were expecting to receive.

If you are not satisfied with the Union's proposed resolution of your complaint, you have the right to contact the information commissioner's Office. Further information can be found on the information Commissioner's website at www.ico.org.uk or via their helpline on 0303 123 1113.