University of Nottingham Students' Union
Data Protection & Information Security Policy

1. Introduction and Basics

Purpose

The University of Nottingham Students' Union (UoNSU/The Union) is committed to the protection of the personal data of students, employees, suppliers and other individuals whom we might hold information about.

The General Data Protection Regulations (GDPR) and the Privacy of Electronic Communications Regulations (PECR) are the two main sets of main laws governing how we handle data. To this end every individual employee, student volunteer, member, or contractor handling data collected or administered by the Union must take responsibility and due consideration for its appropriate use in line with this policy. Any deliberate breach of the data protection policy may lead to disciplinary action being taken and the legal liability for a breach can extend to both the Union and Individuals.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Manager at OS-SUDataProtection@Nottingham.ac.uk.

Controllers and Processors

UoNSU is the *controller* for data collected and used for its services and activities as we determine how and where it is processed. As a controller the GDPR places specific legal obligations on the Union; for example, we are required to maintain records of personal data and processing activities. The Union could have legal liability if we are responsible for a breach and this can extend to individuals.

A *processor* is an individual or company responsible for processing personal data on behalf of the controller – for example our membership database provider (currently MSL), and our finance system provider (currently Exchequer), amongst others. We are also not relieved of obligations where a processor is involved – the GDPR places further obligations on us to ensure our contracts with processors comply with the GDPR.

Personal Data

The GDPR applies to 'personal data' and this is any information relating to an identifiable person.

This definition provides for a wide range of information to constitute personal data, including name, student identification number, location data or online identifier.

The GDPR applies to both automated personal data and to manual filing systems (where there is a logic to the filing).

Special Categories of Data

There are special categories of data, previously known as sensitive data, which require special measures of risk control to be in place. Data falling within this category is:

- Biometric information;
- Genetic information;
- Racial or ethnic origin;
- Political opinions;
- Religious or other similar beliefs;
- Membership of trade unions;
- Physical or mental health or condition; and
- Sexual life
- Sexual Orientation
- Gender

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Principles of Data Processing

Under the GDPR, the data protection principles set out the main responsibilities for organisations. These principles require data to be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is 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; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

There is an additional duty imposed on data controllers that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.” The Union ensures compliance through the training, procedures and policies in place relating to data processing and information security.

Freedom of Information Act

The Freedom of Information Act 2000 ("FOI Act") only applies to public bodies and as the University of Nottingham Students' Union is not a public body we do not respond to FOI requests. Any FOI requests which come into the Students' Union should be forwarded to the Data Protection Manager for review and response.

2. Responsibilities

Staff members

The Union holds various items of personal data about its employees which are detailed in the relevant privacy notice at https://www.su.nottingham.ac.uk/privacy. 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 the HR team and/or updating self-service systems as appropriate.

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 read and understood this policy and when handling personal data staff are required to follow the guidance set out in this policy.

Managers and project leads

Union managers and project leads 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 guidance set out in this policy. Managers are also required to consider their relevant spaces and IT infrastructure to identify weaknesses in information security on at least an annual basis. This will be coordinated centrally by the Data Protection Manager.

Data Protection Manager

The CEO is UoNSUs nominated Data Protection Manager (DPM). The DPM is responsible for ensuring UoNSU carries out its duties around Data Protection. These responsibilities include:

- Informing and advising the organisation, including the Trustee Board and its employees, about their obligations to comply with the GDPR and other data protection laws
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (students, employees, customers etc)
- Monitoring compliance with the GDPR and other data protection laws, including:
    - managing data protection activities and policies
    - advising staff on data protection issues
    - training staff and conduct internal audits as appropriate

- approving unusual or controversial disclosures of personal data
- approving contracts with data processors

The Data Protection Manager shall be assigned the OS-SUDataProtection@nottingham.ac.uk email address.

Trustee Board

The 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 Trustee Board should seek assurance from the Senior Leadership Team that effective arrangements are in place and are working through the Reporting and Finance sub-committee.

3. Compliance

Lawful Data Processing

The Union shall only process data within the law and must make a record of the lawful justification within the relevant privacy notice. In many cases this lawful reason for processing is:

- our legal obligations under the Education Act 1994 and/or Companies Act 2006
- it is in our legitimate interest and we are using individual's data in ways they would reasonably expect and which have a minimal privacy impact

Where consent is obtained then it must be freely given in a very clear and specific statement and the documented consent must be retained as evidence. 'Opt outs' and the use of pre-ticked boxes are **not** allowed. If you plan to use consent as the lawful basis for processing please see the Data Protection Manager.

When processing data you must make sure that you are only using it for the specific purposes notified to the individual when the data was first collected. If you are planning on processing personal data for a new purpose, i.e. using it for something we haven't done before, then you will also need to ensure that we have an appropriate lawful reason for processing the data.

As part of data protection by design, before undertaking a new project where personal data is to be collected and/or processed a 'privacy impact assessment' must be completed in the planning stage of the project to help you identify and minimise the data protection risks of a project. We will also need to establish the lawful basis for processing the data.

In either of the above scenarios, please contact the Data Protection Manager for more information.

Processing Special Categories of Data

UoNSU shall only process special categories of data linked to individuals, such as health data, religious and sexual orientation, where:

- The Union has the consent of individuals except for where the disclosure is to preserve life or for legal purpose.
- Processing is necessary for the establishment, exercise or defence of legal claims

This data may be analysed in broad terms where no direct link to an individual can be made.

Children

Union staff and volunteers shall not process data related to any individual aged 13 or under without the approval from the Data Protection Manager. Should any data be processed for individuals aged 13 or under parental consent will be required in advance of any processing.

4. Respecting Individuals Rights

The GDPR provides clear rights for individuals and the consequences of getting data processing wrong are potentially significant. It can erode trust in our organisation from our members and partners, damage our reputation but also leave the Union and those who have inappropriately handled the data open to substantial fines.

Rights to be informed – Privacy Policies

The right to be informed encompasses our obligation to provide 'fair processing information', which is done typically through a privacy notice. It emphasises the need for transparency over how you use personal data. Our privacy notices are published online at https://www.su.nottingham.ac.uk/privacy for Students, Employees, Suppliers and Contractors. These give individuals information about the collection and use of their personal data. New students are emailed once we start processing their data to make them aware of our privacy policy.

Right to access data

An individual has a right to request the personal data that an organisation holds about them. They also have a right to know the source of the data, the purposes that it is being held for e.g. to process an individual's membership and who it has been shared with.

Individuals can make a request orally, or by email but where possible individuals should complete a ***Subject Access Request Form*** so we have a proper record of the request. See below.

Right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Individuals should in the first instance contact their main SU contact who can most effectively make the change. Alternatively, requests can be made to the Data Protection Manager.

Right to erasure

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. Data can be erased providing that:

- it is no longer necessary for the purposes for which it was collected
- they exercise their right to object to processing of their personal data and there are no overriding legitimate grounds for processing
- the data is unlawfully processed
- the data needs to be erased to comply with legal obligation

Where we have disclosed the personal data in question to third parties, we will inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The right to restrict processing

Individuals have a right to ask us not to process their personal information for marketing purposes. The easiest way for individuals to do this is to use the *unsubscribe* link at the bottom of any marketing email sent out.

In addition, individuals can ask us not to process their personal data where it is processed on the basis of legitimate interest provided there are no compelling reasons for that processing. The compelling reason may be that we are required to process their data by law or that we would be unable to provide any of the membership services without being able to do so.

The right to object

Individuals have the right to object to processing. As with erasure and restrictions, objection to processing may result in the limitation of service provision.

The right to data portability

The right to data portability allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. This right applies where processing is carried out by automated means and the legal basis for processing is consent or contract (which is rare in the SU).

Subject Access Requests

This can be found at https://www.su.nottingham.ac.uk/privacy/ and is the preferred way in which requests should be made. Ideally this should be posted to the Data Protection Manager, University of Nottingham Students' Union, Portland Building, University Park, NG7 2RD.

Individuals requesting access must also provide some form of identification, and information about the data they are seeking. This is to ensure that we only provide information about the person making the request to that individual.

Proof of identity should include a copy of two documents such as birth certificate, passport, driving licence, official letter addressed to the individual's address e.g. bank statement, recent utilities bill or council tax bill. The documents should include their name, date of birth and current address.

Data we need to provide can include:

- Details held on the membership system including notes
- Case files including handwritten notes, emails, letters etc
- CCTV footage
- Photographs
- Records of any contact with the Union
- Complaint files
- Market research activity
- Records of third parties the data is shared with

The scope of the search includes all Union internal and external activities including the commercial element and any other organisation which is processing data on the Union's behalf. It is important to note that email and hardcopy exchanges between SU staff or other individuals may have to be considered for disclosure in response to a SAR. So please:

- Keep any documented information factual
- Carry out periodic housekeeping on email and other information sources as necessary
- Keep a file note of the source of any incoming information (it helps when dealing with a subject access request to know if the requestor already has a copy of the document)
- Only copy into emails those people who "need to know"
- Do not include any personal opinions in email or other documents

Time frame for rights

The GDPR guidance give a very strict deadline of responding to individuals exercising the rights mentioned above within 1 month. **Any individual or department receiving a Subject Access Request, or other rights request, must share this with the Data Protection Manager within 5 working days.** Unlike previous regulations a fee cannot be charged for the subject access request.

5. Information Security

This policy runs alongside the IT Information Security Policy of the University of Nottingham which can be found at https://www.nottingham.ac.uk/it-services/documents/about/security-policy.pdf.

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, must be stored in a locked office or locked storage unit. When no longer needed, the e-copies should be deleted and any paper copies securely destroyed.

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.

Where data is not retained in a dedicated and secure system (such as MSL), the Union has 2 primary platforms for securely storing data online - University of Nottingham Network Drives (S drive and Z drive),

and the University of Nottingham 'One Drive' within Office online. Staff and Volunteers are required to store any personal data they handle on these platforms only.

Restricted information processed on portable devices and media (including stored locally on a laptop/desktop 'C' drive) must be encrypted. The password to an encrypted device must not be stored with the device.

Disposing of IT equipment
Even if you think you've deleted data from your computer it's likely remaining somewhere in some form, so disposing of IT equipment securely is essential. You must contact the Information Services Help Desk to have IT equipment removed and disposed.

Data Retention and Disposal

The Union is committed to keeping data for the minimum time necessary to fulfil its purpose and as a general principle all data should be deleted when it no longer becomes necessary. Core retention periods are as follows:

Data Type	
Membership	In general personal data should be deleted 3 years after the summer in which the student leaves the University. Our policy in MSL is to: - anonymise the data 3 years after the summer in which the student leaves the University - delete the data 6 years after the summer in which the student leaves the University. Other data can retained for longer periods providing it is anonymised and there remains a valid need to retain it. Ask the Data Protection Manager for clarification if this applies.
Elections data	1 year
Student Advice Centre	6 years
Employee	Recruitment information retained for 6 months from date of interview. Most other data will be removed after a minimum of six years after their employment with the Union has finished, in order to meet data needs for pensions, taxation, potential or current disputes, or job references.
Business and financial records	6 years
CCTV	30 days
Health and safety information	3 years, unless required by law to retain for longer periods (e.g. if the accident involves someone aged under 18, the records are retained until 3 years after their 18th birthday)

Market research	TBC

Paper based records shall be disposed of in a confidential waste sack, confidential waste bin, or shredded. Electronic records will be deleted through the decommissioning of equipment by the University Information Services department and digital records shall be deleted from databases at source.

Third Party Contracts

Occasionally the Union may transfer data to third parties for processing. Prior to data transfer a contract to ensure compliance with relevant legislation must be in place. Particular attention needs to be given to any third party based outside of the EU with oversight of this being required by the Data Protection Manager.

Information Security Breaches

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking attack
- Deception of the organisation through 'blagging' offences

Detecting data breaches
Detecting a data breach or the potential of a data breach can happen in a variety of ways. The table below identifies some of the methods of detection and processes for handling such detections.

Detection Method	**Action for potential breach**	**Action for actual breach**
Employee/ Volunteer Detection	If you think you have identified a potential for data security to be breached you must immediately inform your line manager (or staff contact if you are a volunteer) and the Data Protection Manager. They may immediately cease processing this data until the potential for breach is resolved based upon an assessment of the risk to individuals privacy.	Immediately report the matter to the Data Protection Manager, permanent staff contact (if volunteer) or line manager - isolating any potential for further breach where appropriate. The DPM and other involved parties should follow the CIRP detailed below.
Accidental Breach (such as loss of laptop)	The SU has laptop locks to reduce the risk of theft when working outside of access controlled offices. Always ensure data is secured and encrypted as detailed in the	Immediately report the matter to the Data Protection Manager, permanent staff contact (if volunteer) or line manager -

	data storage section of this policy. Consult the Data Protection Manager or line manager where appropriate.	isolating any potential for further breach where appropriate. The DPM and other involved parties should follow the CIRP detailed below.
Complaint from either an individual, organisation or legal representative	Where there is a risk of complaint arising from the processing of data that may give rise to a legal matter processing must immediately cease, the DPM and relevant member of the Senior Leadership team must be advised.	Immediately report the matter to the Data Protection Manager and member of the Senior Leadership team. The DPM and other involved parties should follow the CIRP detailed below.

Reporting data breaches
Where an employee, volunteer, supplier or contractor discovers a data breach they must report this to the Data Protection Manager within 24 hours of first becoming aware.

The Information Commissioner's Office (ICO) shall be notified within 72 hours of first becoming aware 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 economic or social disadvantage. The Data Protection Manager has responsibility for informing the ICO and this may be delegated to other members of the Senior Leadership team. Where necessary, legal advice should be obtained.

Where there is a high risk to the rights and freedoms of individuals they shall be notified directly also as detailed in the ***Cyber Incident Response Plan*** outlined below. Responsibility for this also falls to the DPM.

Investigating data breaches
The Union takes all data breaches seriously and will investigate all potential and actual data security breaches. The process for actual data breaches is outlined below in the ***Cyber Incident Response Plan***.

Cyber Incident Response Plan
In the event of a data security breach the Data Protection Manager shall coordinate the Cyber Incident Response Plan outlined below:

Containment and recovery
The following activities must be completed within 72 hours of any breach notification:

- The DPO shall identify the appropriate specialist, either internal or external to investigate the breach and ensure that they have the appropriate resources
- The investigating party shall establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating a piece of equipment, finding a lost piece of IT hardware or simply changing the access codes to a certain space.

- The investigating party shall also establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause, as well as the physical recovery of equipment. Where appropriate the police should be informed.

Assessing the risk

Some breaches may be minor and not lead to risks beyond an inconvenience, however some breaches, such as theft of a customer database with which identity fraud could be committed, are much more serious. Before deciding what steps to take beyond immediate containment there must be an assessment of the risk. The investigating party should assess:

- What type of data is involved?
- How sensitive is the data?
- If the data has been lost or stolen are there any protections in place such as encryption
- What has happened to the data and could it be used of purposes harmful to individuals
- Regardless of what has happened to the data, what could the data tell a third party about an individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there wider consequences to consider such as a loss of public confidence?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice.

Notification of breaches

Where appropriate, it is important to inform people and organisations of a data security breach. Informing people about a breach is not an end in itself. Notifications should have a clear purpose to either allow the ICO to perform its function, provide advice, deal with complaints or enable individuals to take steps to protect themselves.

- The Data Protection Manager shall identify if there are any legal or contractual requirements to comply with in the event of a security breach
- The Data Protection Manager shall identify whether to notify the affected individuals by considering the risk to those individuals and the part they can play in mitigating those risks - such as changing passwords or changing building access codes. The investigating party should also consider the risks of over notifying - where 200 members of a student group are affected, a notification to the 23,000 members of the Union would be disproportionate.
- If notifying individuals there should be specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them.
- The Data Protection Manager shall work to identify whether the Information Commissioner's Office needs notifying. Notifications to the ICO should include details of security measures in place, security procedures in place and the time of the breach.
- The Data Protection Manager should also consider what third parties, such as the University, police, insurers and professional bodies, require notification. The Union has an insurance policy that provides specific legal and data breach support.
- Legal advise should be obtained as necessary.

Evaluation and response

It is important not only to investigate the causes of the breach but to evaluate the effectiveness of the organisations response to it and the measures in place to prevent it happening again. The Data Protection Manager shall curate an evaluatory body of relevant employees and/or volunteers to ensure procedures, policies and equipment is of sufficient security standard to avoid future breaches in this mechanism.