DURHAMSU

Data Protection Guidelines

Reviewed 21/06/18

1. Introduction to this handbook

Data protection law in the UK and Europe is being strengthened. This makes it even more important, for the Students' Union and our members, that privacy is integrated into our day to day work. The increasing profile of the importance of protecting personal data means that the public at large, and so also both our current and potential members, are more conscious of it. We cannot afford data protection to be an afterthought.

With this in mind, this handbook has been designed to give employees and volunteers who handle data an appreciation of the legal requirements that the Union must abide by to ensure that they comply with the General Data Protection Regulations.

The Students' Union needs to collect personal information about people with whom it deals in order to carry out its business and fulfil its charitable objectives. Such people include students, employees (present, past and prospective), suppliers and other business contacts. This information includes name, address, email address, dates of birth, private and confidential information and occasionally sensitive information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law.

No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hard copy, paper or images) this personal information must be dealt with properly to ensure compliance with the EU General Data Protection Regulations (GDPR).

Contents

Contents

2. Introduction to the regulations

General Data Protection Regulations

The European Union legislation known as the General Data Protection Regulations (GDPR) is enforced from the 25th May 2018. This handbook, associated policies and procedures are all designed to ensure compliance with these regulations.

Controllers and Processors

Durham Students' Union is the controller for data collected for its services and activities whereas Durham University is the data controller of student records forming our membership records.

A processor is an individual or company responsible for processing personal data on behalf of the controller - for example student groups, National Governing Bodies and our electronic point of sale systems. The Students' Union is also a processor when handling membership records provided to us by Durham University.

As a processor the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach, which can extend to individuals.

However, controllers are 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.

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU. For example, we use Google Analytics, and Google is therefore required to be GDPR compliant.

Personal Data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, student identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

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.

Please note: from information provided, there is no evidence that by joining a specific club or society the student is providing information about any special categories of data. For example, a student joins the LGBT+ Association, any information about their sexuality or beliefs would be an assumption only, and would not qualify under this category.

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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; 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 Students’ Union ensures compliance through the training, procedures and policies in place relating to data processing and information security.

Individual's rights and freedoms

The GDPR provides the following rights for individuals - this part of the handbook explains these rights and our standard organisational response to these rights when processing data.

The right to be informed – collecting data

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. The Union publishes privacy notices at durhamsu.com/privacy.

The right of access – collecting data

Individuals have the right to access their personal data and supplementary information which allows them to be aware of and verify the lawfulness of the processing. Individuals requiring access to the data the Union holds on them must complete a ***Request Your Individual Data Form***.

The Union must respond to these requests within one month; therefore any staff member or volunteer receiving a Subject Access Request Form must send this to the Data Protection Officer within five days of receipt to ensure they can coordinate the collection of the individuals' data within the timeframe.

The right to rectification – using data

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. It's vital that we retain a clear trail of where information has been disclosed to third parties as we must inform them of the rectification, where possible.

As with the right of access the Union must respond within one month of receipt of a ***Request to Change Your Data Form***. Any employees or volunteers receiving a Data Rectification Form must send this to the Data Protection Officer within 5 days of receipt to ensure they can coordinate the rectification of the individuals' data within the timeframe.

The right to erase

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.

A large majority of data the Union processes relates to the delivery of service - individuals must be informed that erasing their data will not only mean inability to serve them but if complete erasure from Union records is required then this will result in termination of membership. Individuals should be directed to the ***Request the Erasure of Your Data Form*** which should be sent to CEO Gareth Hughes, the Data Protection Officer to coordinate the administration of the erasure. Requests for erasure are to be fulfilled within 30 days of the request, unless the request is onerous.

If you have disclosed the personal data in question to third parties, you must 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 – using data

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. An example would be members opting out of receiving email communications.

For data processing activities such as mass email communications the Union provides automated opt-out systems which the individual can use to limit our processing. For processes where automated systems are not available individuals should be directed to the ***Request to Restrict the Processing of Your Data Form*** which should be sent to the Data Protection Officer to coordinate the administration of. As with erasure, restrictions of processing may result in the Union's inability to serve the individual with a specific service or activity, and where third parties have been shared with this data they must be informed of the restrictions.

The right to data portability – using data

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The Union collates and provides data in CSV formats. Individuals can request their data using the ***Request Your Individual Data Form*** and employees and volunteers should respond to these requests in the same time frame as the access requests detailed previously.

The right to object – using data

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

Much of the Union’s data processing activities are based on legitimate interests, research or direct marketing so it’s important that employees and volunteers are aware of this right. As with erasure and restrictions, objection to processing may result in the limitation of service provision. The process identified for restriction should be followed for objections.

Rights in relation to automated decision making and profiling – using data

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. The Union does not make automated decisions about individuals that may be damaging without any form of human intervention.

Privacy and Electronic Communications Regulations

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection regulations. They give people specific privacy rights in relation to electronic communications. There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

The ICO has several ways of taking action to change the behaviour of anyone who breaches PECR. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner can also serve a monetary penalty notice imposing a fine of up to £500,000.

The key requirement of the PECR is that individuals contacted by these methods must have given their prior consent other than in very limited circumstances. PECR does not consider that contacting people as a default unless they have opted out is satisfactory. They look for evidence that individuals have given their explicit consent before any communications take place. This can make contacting potential members and members tricky when it comes to information which is about educational and campaigning matters.

Soft opt-in consent is only acceptable when the following three criteria are met:

1. The contact details were obtained from the individual during a sale or negotiation of a sale for a product or service. For the Students' Union this will usually be when a person is becoming a student group member or we are contacting an existing group member; and
2. The communications relate to similar products or services; and
3. The option to opt out (or "unsubscribe") was provided when the data was collected and is included on each and every subsequent communication

The conditions are specific and so cannot be relied upon in many situations. Difficulties can arise when using a member's mobile or home telephone number to send campaigning messages if the number was not initially collected for the purpose of campaigning; instead, for example, during registration as a volunteer driver or purchasing tickets.

It is therefore very important to know why the personal data that you have was collected in the first place. This detail can be found by reviewing our Data Process Matrix, which is kept up-to-date by team managers and provides oversight to our Data Protection Officer, CEO Gareth Hughes.

Freedom of Information Act

The Students' Union, although a representative body for students at a publicly funded institution, is not itself a public body. The Freedom of Information Act 2000 ("FOI Act") only applies to public bodies. Any FOI requests which come into the Students' Union should be forwarded to the Data Protection Officer for review and response – the standard response is that the FOI Act does not apply to the Students' Union and therefore the information will not be provided.

Individual responsibilities

All individuals handling data on behalf of Durham Students' Union have a responsibility for compliance with these procedures. An overview of responsibilities is contained within the Union's ***Data Protection & Information Security Policy***.

Data can only be processed if there is a legal basis for doing so. All staff involved in processing data must be aware of what this legal basis is.

- ICO advice about the legal bases for processing data
    - Consent - The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis
    - Contract - if you need to process someone's personal data to fulfil your contractual obligations to them or because they have asked you to do something before entering into a contract, e.g. provide a quote
    - Legal obligation - if you need to process the personal data to comply with a common law or statutory obligation. This does not apply to contractual obligations
    - Vital interests - if you need to process the personal data to protect someone's life
    - Public task - if you need to process personal data 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or to perform a specific task in the public interest that is set out in law.
    - Legitimate interests - where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing
- If you are processing special category data you have identified a lawful basis (see above) AND a separate condition for processing special category data
- If another organisation is collecting the data for you, or you'll give the data to another organisation to process you have a suitable contract in place

Before **collecting** any data for processing in a new way/manner the following process and forms must be completed and agreed by the Data Protection Officer:

- Entered, with all columns complete, in the Date Processing Matrix and approved by Manager, including;
- Reviewing if a Privacy Impact Assessment Form is required
- Reviewing if a Legitimate Interest Assessment Form is required
- Completing a Data Collection Assessment Form

The consequences of getting data processing wrong are substantial. Not only can it erode trust in our organisation and damage our reputation but it may also leave the Union and those who have inappropriately handled the data open to substantial fines under the GDPR. Article 83(5)(a) states that infringements of the basic principles for processing personal data, including the conditions for consent, are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

Where employees who handle data will be unable to access and read emails for longer than 3 working days they must display the following notice on their out of office to ensure that individuals

requesting access, rectification or removal to their own data are responded to within the appropriate timescale:

> *Requests relating to data protection should be sent to the Data Protection Officer, CEO Gareth Hughes, by email to su.admin@durham.ac.uk.*

Where the data protection officer is not able to respond to enquiries within the given timeframe due to extended leave, sickness, or any other reasonable reason an appropriate person within the organisation must be delegated authority and responsibility to handle data protection enquiries.

3. Key activities & data protection procedures

Employee Administration

This section covers data processing activities relating to how the Union handles employee data for administration purposes.

Recruitment

Potential employees' personal data can be collected as long as the people are aware their data is being recorded and retained. It is imperative that the data collected about potential members is not excessive – avoid collecting more information than is needed – and that it is stored securely and not shared with anyone who has no need to see it. A retention period should be set for this information and, once this time period has elapsed, the data should be disposed of securely i.e. deleted from a computer or shredded or placed in a confidential waste bin or bag if it is in paper form.

Employee Records

When starting employment with the Students' Union employees sign a contract which provides consent to process personal information, sensitive information and transferring this data in the delivery of services such as payroll, insurances and for advice. A retention period is set within the employee privacy statement, once this time period has elapsed, the data should be disposed of securely i.e. deleted from a computer or shredded or placed in a confidential waste bin or bag if it is in paper form. Employees have a responsibility for ensuring their data remains up to date.

Membership Administration

This section covers data processing activities relating to how the Union handles membership data for administration purposes.

Students' Union Membership Records Data Set

Annually Durham Students' Union forms registration contracts with students. This contract includes the option for membership of the Students' Union. This contract is annually created with each member and provides the rights for the University to transfer the Membership Records to the Students' Union. This transfer includes detailed limitations for processing of this data. The Students' Union then collects and renews data from the University several times through the year to ensure this data is accurate.

These records are managed by the Students' Union marketing department and direct access to this data is restricted to this department and the insights function only. The Students' Union marketing and communications team will send an **activation of membership email** to all members prior to any further marketing communication.

Student Groups Membership Data Set

The Students' Union provides a membership management platform that facilitates both paid and free memberships of student groups. Volunteers running student groups are strongly advised not collect data externally from this system. This restriction is in place to ensure that individuals are aware of the privacy notices which indicate how their data will be processed.

- Employees and volunteers will be assigned specific access levels to handle certain data to administer student activities using the membership platform;

- Volunteers must complete data protection training before being provided with this access and as a result may not re-assign authority and access without formal agreement from the Data Protection Officer;
- Employees are bound by policies and procedures and may not re-assigned access rights without formal agreement from the Data Protection Officer;
- Employees and volunteers may not transfer data to third parties without the explicit consent from the individual students to facilitate this the Union's membership platform allows students to consent to this exchange;
- Access levels are assigned by the marketing and communications team; and
- The data may only be processed for the purposes outlined in the **Data Collection Assessment Form** available to Durham SU staff on the S Drive, employees and volunteers must be careful to only use personal data for the purposes that are outlined in this document.

If you wish to use this data for any purpose other than what has been declared on the **Data Collection Assessment Form and Data Processing Matrix** (found on the Durham SU S Drive) then you must consider this a new use and follow the procedures set out below for collecting data or using third party data - in particular the Privacy Impact Assessment.

Using Data Extracts From the Membership System

Data extracts from the membership system must only be used in line with the appropriate processing activities set out in the **Data Collection Assessment Form**. Employees and volunteers processing the data must ensure that the information is:

- Not circulated widely;
- Only made available to authorised data handling individuals;
- Only used for the specific purpose for which it was collected;
- Held securely (password protected); and
- Securely destroyed after use.

Below is a table of things to do and not do, which should be kept in mind when processing data from membership systems.

Do	**Do Not**
Only extract and use the information that is needed to complete a task	Extract more than you need for a task. A lack of time is not a legitimate reason for not considering the exact data needed.
Keep the information on systems and networks that are recognised as being acceptable for Union and University work such as University networked equipment (S drive)	Email information to a personal email address or save it onto a personal device for any reason
Take care when taking personal data out of the Union Buildings. Only take the information if it is necessary, keep it safe and return it as soon as possible.	Keep the information that you have got to use for a very similar exercise that you know you're going to do in the future
Update the relevant staff member responsible for the data if an individual's information is out of date.	Leave personal data that has been taken out of the office unattended
	Put information into a normal bin - use a secure disposal bin or bag. Someone else

	could find it and misuse it
	Provide information to others not involved in the task for which the data was extracted

Data Cleansing

This is a crucial activity in the run up to Freshers and elections processes. It is natural for members to leave, change course, or change status and it's therefore vital the Union cleanses its data regularly.

There are processes for the removal of members in specific scenarios:

- **Removal of membership rights**
  Where disciplinary processes, or opt-out processes, result in the removal of a member from the Students' Union, the Chief Executive shall share the name and student ID with relevant departments to ensure removal from Union databases. The Chief Executive shall also ensure that any student groups and third parties who process the individuals' data are informed.

- **Death of a member**
  Where a member is deceased it is vital their data is removed from Union systems to prevent unrequired communication that may distress relatives. The Students' Union Chief Executive shall share the name and student ID with relevant departments to ensure removal from Union databases. The Chief Executive shall also ensure that any student groups and third parties who process the individual's data are informed.

Membership Communications

Contacting members for some activities by email or text message requires specific opt-in consent. Article 47 of the GDPR states that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or member. A ***Legitimate Interest Assessment Form*** should be completed for membership communications to ensure balancing of the interests of the data subject.

Emailing and text messages

The ICO has stated that all email addresses are personal data; it is therefore essential that when bulk communicating with members using email distribution lists that the following provisions are made:

- Individuals who have opted out of mailings (apart from statutory information like voting information) are not included in mailings or bulk text messages (this is still required in instances of legitimate interest);
- The blind carbon copy (Bcc) field on the email address line is used. If you're unsure on how to use this when sending an email, ask an additional member of staff who will be able to help;
- If a member informs the Union that they no longer wish to be contacted via email or text, their name and contact details must be removed from the distribution list, and a note made that they have not consented to receive emails or texts. The only exception to this is if the message contains statutory Union information and cannot be provided to the member in another way.

- An option to unsubscribe to similar communications is added to the bottom of the email or text message each time a message is sent out.

Note: Communications with generic @durham.ac.uk addresses such as society.name@durham.ac.uk are not considered personal data as they do not identify an individual.

Supporting platforms

The Marketing team are responsible for providing, maintaining and monitoring platforms which facilitate the communication with members.

For employees, there is:

- A bulk email platform to which access is strictly limited to authorised staff

For volunteers, there is:

- A member messaging platform built into the membership platform for messaging members of the group(s) that they administer

Commercial Marketing

Soley purposed commercial marketing, through email or SMS, must only be delivered to those who have opted-in to receive commercial marketing messages. Fundraising through commercial activities is vital to the success of the organisation and therefore employees and volunteers collecting data should make commercial message opt-in options available at all appropriate opportunities.

Commercial marketing messages must include an opt-out function and may be considered a legitimate interest where a commercial relationship already exists as detailed above. For example if student purchased a Freshers' Week ticket it could be assumed that they have provided soft opt-in consent to contact them regarding a Christmas Ball and Graduation Ball.

Representing Members

Advice and representation cases

This section covers data processing activities relating to how the Union represents its members - in particular in handling case files. Any information directly related to a potential or actual case is extremely sensitive and several of the data protection principles apply.

Provisions that representatives and advisors need to make include:

- Secure storage for live and archived case files
- Limited access to only those officials who need to see the data
- Collection of data limited to only that which is relevant to the case in hand
- Information held in the file is accurate
- A sign in/out process if the file needs to be taken out of the Union's office space
- File retention policy
- Secure disposal

It is much safer to keep any case files within the Union Building. If this is not possible, i.e. a file needs to be taken off the premises considerable care should be taken to ensure that its whereabouts are known, and that it is always kept secure.

Democratic platforms
The Union is legally obliged by the Education Act 1994 to engage and facilitate students in elections processes which requires processing specific data. The data used for this activity is the membership data provided by Durham University.

For campaigning and lobbying activities the Union requires consent to process the data - this is because individuals personal data is made publicly accessible during many of the functions and a legitimate interest balance may not be achieved. Consent statements are detailed within the ***Data Collection Assessment Forms*** and must be displayed at the point of system engagement.

As with all forms of data collection a retention period must be clearly established and data securely deleted by the parties controlling the platforms the data is held within at the point this period expires.

Research & Insights

This section covers data processing activities relating to how the Union undertakes research activities.

The Students' Union insight gathering activities, such as surveys are undertaken by consent. Records of individuals views, unless anonymised, are considered personal data and as such are subject to the rights and freedoms detailed previously in this handbook.

Data published must not individually identify any person without their explicit consent however anonymised data from all datasets maybe be processed and published for statistical purposes. Data should only be collected through the agreed platforms and by authorised individuals.

As with all forms of data collection a retention period must be clearly established and data securely deleted by the relevant employee/team at the point this period expires.

Service Administration

This section covers data processing activities relating to how the Union delivers administration of services for members, suppliers, contractors and visitors. This data can include:

- Bank account details for the purpose of making payments
- Commercial clients for the purposes of credit control and management
- Drivers details for insurance purposes
- Events customers for the purposes of ticket management
- Retail customers for the purposes of fulfilment, delivery and order management

Employees and volunteers processing this data must ensure that the information is:

- Not circulated widely;
- Only made available to authorised data handling individuals;
- Only used for the specific purpose for which it was collected;
- Held securely; and
- Securely destroyed after use.

Third Party Data

Where the service uses Third Party data to facilitate the service administration there must be a declaration of its use to the individuals whose data is being processed. This must be delivered within one month of obtaining the data, at the point of first communication or prior to disclosure to any further parties. Should the third party notify the Union, or the Union become aware, of any errors in data this must be rectified within one month of notification.

Third Parties requiring the erasure of data or applying restrictions in processing are required to notify the Data Protection Officer who will, subject to our rights to refuse, undertake all reasonable procedures to ensure the erasure of the individual's data from Union records. Where the Union's Data Protection Officer advises employees or volunteers of a restriction or erasure notice you are required to abide by this notice.

4. Information security procedures

Data storage

Hard copies, file notes, incoming and outgoing letter correspondence
The Students' Union has a duty to ensure that data is held securely. Provisions that employees and volunteers must consider putting in place include:

- Lockable filing cabinets
- A clear desk policy
- Secure storage for archived files
- Secure destruction: using a shredder or confidential waste bin

Electronic Data

The same requirements apply to electronically held data. Provisions employees and volunteers must consider putting in place include:

- Use storage on the University network, or approved platform
- Password protection on all files containing personal data
- Use of the Union's secure platforms for processing data
- Up to date antivirus and malware systems
- Adequate firewalls
- Secure destruction of IT equipment

Disposing of IT equipment

Even if you think you've deleted data from your computer its likely remaining somewhere in some form, so disposing of IT equipment securely is essential. You must contact CIS to have IT equipment removed and disposed.

Email Security

Your @durham.ac.uk account is individually assigned to you and should not be shared with others. You should take the following steps to ensure the security of your email content:

- Consider whether the content of the email should be encrypted or password protected. If sending a spreadsheet containing personal data this must be password protected and the password sent in a separate email.
- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Dave's". Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- Never click on a link or share any information with anyone that you don't recognise - if in doubt check with another member of staff who may be able to help.

Sharing information

Whenever the Union uses a third party processor we must to have a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities. As the controller for certain elements of data the Union is liable for ensuring our compliance with the GDPR and we must only appoint processors who can provide sufficient guarantees that the requirements of the GDPR will be met and the rights of data subjects protected.

Third party processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

Releasing information to prevent or detect crime

The police or other crime prevention/law enforcement agencies sometimes contact data controllers or data processors and request that personal data is disclosed in order to help them prevent or detect a crime. All such requests must be referred to the Data Protection Officer.

The Students' Union does not have to comply with these requests, but the regulations do allow organisations to release the information if they decide it is appropriate. Before any decision is made about disclosure, the Information Commissioner asks that organisations carry out a review of the request. This include considering:

- The impact on the privacy of the individual/s concerned
- Any duty of confidentiality owed to the individual/s
- Whether refusing disclosure would impact the requesting organisation's ability to detect, prevent or prosecute an offender

If a decision is made to refuse, it is possible that a subsequent court order may be made by the requesting organisation for the Students' Union to release the information. If such a request is received by an employee or volunteer, please refer the requestor to the Students' Union's Data Protection Officer.

Information security breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

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 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) and the Data Protection Officer. 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 Officer, permanent staff contact (if volunteer) or line manager - isolating any potential for further breach where appropriate. The DPO and other involved parties should follow the CIRP detailed below.
Accidental Breach (such as loss of laptop)	If there is a high likelihood of this breach happening you should immediately adjust your processes and procedures to reduce the likelihood. Always ensure data is secured and encrypted as detailed in the information security section of this handbook. Consult the Data Protection Officer or line manager where appropriate.	Immediately report the matter to the Data Protection Officer, permanent staff contact (if volunteer) or line manager - isolating any potential for further breach where appropriate. The DPO and other involved parties should follow the CIRP detailed below.
Audit or assessment	The Union conducts termly data audits of its spaces and IT infrastructure using the **Office and IT Data Security Assessment** - these may highlight weaknesses in the organisations information security and should be responded (with advice from the Data Protection Officer) in a timely manner to ensure data privacy of individuals.	Immediately report the matter to the **Data Protection Officer**, permanent staff contact (if volunteer) or line manager - isolating any potential for further breach where appropriate. The DPO 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 raise to being a legal matter processing must immediately cease, Senior Leadership Team must be advised and comprehensive guidance sort from the Information Commissioner's Office.	Immediately report the matter to the Data Protection Officer and a Strategic Leader of the Union. The DPO 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 Officer within 24 hours.

The Information Commissioner's Office shall be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals such as discrimination, discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

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.

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 Officer 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.

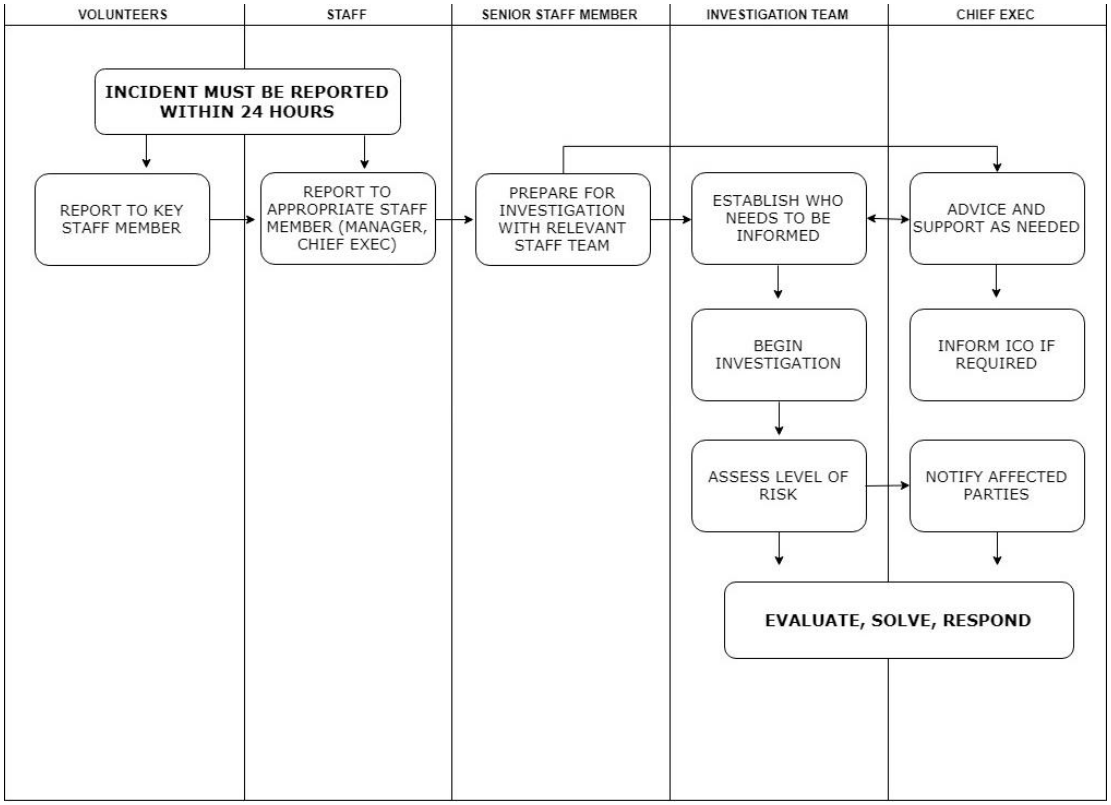
- The Data Protection Officer shall identify if there are any legal or contractual requirements to comply with in the event of a security breach
- The Data Protection Officer shall identify whether to notify the affected individuals by considering the risk to those individuals and the part they can play 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 Officer 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 Officer should also consider what third parties, such as the police, insurers and professional bodies, require notification. The Union has an insurance policy that provides specific legal and data breach support.

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 Officer 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.

Responding to data breaches

Opposite is a diagram of our process for responding to data breaches:



Disposing of data

The Union is committed to keeping data for the minimum time necessary to fulfil its purpose.

- **Member Data** - Member (student) files shall be removed from one year after a student graduates or otherwise leaves the University.
- **Employee Data** – Shall be removed from 3 months after an employee leaves the organisation
- **Health and Safety Data** - The Union will keep health and safety records of accidents that happen to visitors to the Union for three years after the date of accident.

Paper based records shall be disposed of in a confidential waste sack, confidential waste bin, or shredded. Electronic copies or records will be removed from relevant systems and drives where appropriate and deleted from databases at source. Copies and records may also be deleted through the decommissioning of equipment by the University (CIS).

5. Requests for an individual's own data

The rights of the individual
Under the Data Protection regulations an individual has a right to request all 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. The individual needs to make the request in writing by post.

Individuals requesting access must provide some form of identification, and information about the data they are seeking. Subject to the verification of the individual's identity and the specific requirements, within one month of request receipt, the Union shall provide:

- Confirmation that their data is processed;
- Access to their personal data; and
- Other supplementary information as outlined by law

A Subject Access Request (SAR) form must be completed and provided to the Data Protection Officer for distribution of appropriate actions. Any individual or department receiving a Subject Access Request must share this with the Data Protection Officer within 5 working days. The Data Protection Officer must respond to the request within one month of receiving the request and proof of identity.

Data we need to provide can include:

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

The scope of the search includes Union activities, services, central services and trading activities and any other organisation which is processing data on the Students' Union's behalf. It is important to note that email and hardcopy exchanges between Students' Union officials and representatives to each other and to/from regional officers with reference to any representations or issues with members 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 use abusive or derogatory language in emails or other documents
- Do not include any personal opinions in email or other documents
- Do not use email when a telephone call will do

What to do if a request for subject access is received by an employee or volunteer

If a verbal request is received the employee or volunteer should inform the individual that they need to put their request in writing and email su.admin@durham.ac.uk.