DATA PROTECTION AND INFORMATION SECURITY HANDBOOK

Updated: January 2021

BUCKS STUDENTS' UNION

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. 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 provide its services. Such people include students, employees (present, past and prospective), suppliers and other business contacts. This information includes name, address, email address, date 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 (eg on a computer or other digital media, on hard copy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with the EU General Data Protection Regulations (GDPR).

The appendices in this handbook contain further detailed information and example documentation which employees and volunteers will find useful. The content of this handbook is correct at the time that it was issued and will be updated from time to time as privacy legislation changes.

BUCKS STUDENTS' UNION POLICY DOCUMENT

BUCKS STUDENTS' UNION

Contents

1. Quick Reference guidance

I would like to…	Where to look for more information…
Understand my responsibilities for data protection	• Introduction to regulations • Individual responsibilities • A guide to processing special categories
Understand the rights of those who we process data about	• Individual's rights and freedoms • Freedom of Information Act
Respond to a request to access data, erase data, or restrict processing of data	• Individual's rights and freedoms • Individual responsibilities • Requests for an individual's own data
Send electronic marketing or communications messages to individuals	• Privacy and Electronic Communications Regulations • Individual responsibilities • Membership Communications
Undertake a project that collects and processes data	• Individual responsibilities • Information security procedures • A guide to displaying privacy notices • A guide to lawful processing • A guide to processing special categories • A guide to undertaking a legitimate interest • A guide to undertaking a privacy impact assessment
Access and process employee records	• Individual responsibilities • Employee administration • Service administration • Information security procedures
Access and process membership records	• Individual responsibilities • Membership administration • Representing members • Information security procedures • Volunteers as data processors contract
Access and process insights data	• Individual responsibilities • Research and insights • Information security procedures
Release information to third-parties	• Information security procedures • Third-party data sharing contract
Identify and respond to data breaches	• Introduction to regulations • Information security procedures • Data breach flow chart

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 25 May 2018. This handbook, associated policies and procedures are all designed to ensure compliance with these regulations.

Controllers and processors

Bucks New University is the controller for data collected for its services and activities whereas Bucks Students' Union 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 or National Governing Bodies.

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.

The GDPR does not however apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

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 condition
- sexual life
- sexual orientation

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; 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.
- 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

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 **bucksstudentsunion.org/privacy** for students, employees, suppliers and contractors which must be referred to at the point of data collection or when processing third-party data.

The right of access

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 Subject Access Request Form.

The Union must respond to these requests within 30 days of the request. 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 assimilation of the individuals data within the timeframe.

The right to rectification

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 Data Rectification Form. Any employees or volunteers receiving a request to rectify data should contact the Data Protection Officer who will send an electronic copy of the Data Rectification Form and 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 erasure of 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 asked to contact the Data Protection Officer who will be able to send an electronic copy of the Data Erasure Request Form who will coordinate the administration of the erasure. Requests for erasure are to be fulfilled within 30 days of the request.

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

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 being members opting out of receiving email communications.

For data processing activities, such as email, 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 asked to contact the Data Protection Officer who will be able to send an electronic copy of the Processing Restriction and Objection Request Form and coordinate the administration of restricted processing. 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

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 typically provides data in CSV formats. Individuals can request their data using the Subject Access Request Form and employees should respond to these requests in the same time frame as the access requests detailed previously.

The right to object

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 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

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
- 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 member or we are contacting an existing member.
2. The communications relate to similar products or services.
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 driver or purchasing tickets.

It is therefore very important to know why the personal data that you have was collected in the first place.

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.

3. Individual responsibilities

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

Before collecting any data for processing the following forms must be completed and agreed by the Data Protection Officer:

- Data collection assessment form
- Privacy impact assessment form

Where the lawful reason for processing data is identified as a legitimate interest the following form must also be completed and returned to the Data Protection Officer for balancing agreement.

- Legitimate interest 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.

Requests relating to data protection should be sent to the Data Protection Officer by email to **sudataprotection@bucks.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. In these circumstances, any queries should be directed to the Chief Executive Officer or the Deputy Chief Executive Officer.

4. Key activities and 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 ie 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 Data Privacy Statement. Once this time period has elapsed, the data should be disposed of securely ie 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 Bucks New University forms registration contracts with students. This process automatically makes a student a member of Bucks Students' Union, unless they choose to opt-out at enrolment. We believe that the legal basis for having access to this information falls under legitimate interests as our activities and services form a core part of the student experience. When the University gives us this data we become responsible for it and will use this as our core central record of your membership.

These records are managed by the Students' Union Communications and Marketing team and direct access to this data is restricted to this department and the insights function only.

Student groups membership data set

The Students' Union provides a membership management platform that facilitates memberships of various different student groups. When student groups gather additional information at various events, such as freshers' or re-freshers' fairs they will need to ensure they include the relevant statements which will outline the reasons for gathering the information and a link to the relevant privacy statement.

Employees or student groups must not transfer data to third-parties without the explicit consent from the individual students.

Access levels to the membership system are assigned by the Communications and Marketing team and individual users must use their own credentials to login.

The data may only be processed for the purposes outlined in the Data Collection Assessment Form.

If you wish to use this data for any purpose other than what has been declared on the Data Collection Assessment Form 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 inline with the appropriate processing activities set out in the Data Collection Assessment Form. Employees 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
- securely destroyed after use.

Below is a table of things to do and not do, which you should consider 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.
Only use data for one task. A new list should be extracted for each task. This makes sure the data that is being used is up-to-date and accurate.	Provide information to others not involved in the task for which the data was extracted.
Keep the information on systems and networks that are recognised as being acceptable for Union and University work.	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.

Data cleansing

This is a crucial activity in the run up to freshers' and elections processes. It is natural, in an educational landscape, 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 Data Protection Officer shall share the name and student ID with relevant departments to ensure removal from Union databases. The Data Protection Officer 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 Data Protection Officer shall share the name and student ID with relevant departments to ensure removal from Union databases. The Data Protection Officer shall also ensure that any student groups and third-parties who process the individual's data are informed.

Membership communications

As is explained in section two of this handbook (about the PECR), contacting members for some activities by email 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

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, are not included in mailings.
- The blind carbon copy (BCC) field on the email address line is used.
- If a member informs the Union that they no longer wish to be contacted via email, their name and contact details must be removed from the distribution list, and a note made that they have not consented to receive emails. 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 each time a message is sent out.

Supporting platforms

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

Through the website, there is a bulk email platform which is only accessible to the Communications and Marketing team. Where possible, all bulk emails should go through the website to ensure they go to the right audience and that the appropriate links are included to either unsubscribe or view our privacy statements.

It is important to have appropriate systems and checks in place if staff you are sending out emails directly to individuals. This will ensure the right content is being sent to the right individual and that we minimise any potential breach of data. If in doubt, ask the Data Protection Officer.

Commercial Marketing

Solely purposed commercial marketing, through email, must only be delivered to those who have opted-in to receive messages.

Representing members

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 Bucks New University.

For all other democratic processes 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 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 and 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 Communications and Marketing 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 fulfillment, delivery and order management.

Employees 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
- 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 of a restriction or erasure notice you are required to abide by this notice.

5. 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 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, that employees must consider putting in place, include:

- using storage on the University network
- 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 (provided through University IS&T team)
- adequate firewalls (provided through the University network)
- secure destruction of IT equipment.

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. This will most likely be dealt with by the Communications and Marketing Manager.

CCTV recordings

CCTV units are not networked and access to the systems are through password protected platforms. This data may only be accessed by management of The Venue or law enforcement agencies. All CCTV units are subject to the provisions set out in the respective Data Collection Assessment Form.

Email security

Your network login and email account is individually assigned to you and should not be shared with others. In an employee's absence or for specific investigation purposes only emails may be accessed by authorised individuals - authority is granted by a member of the Union's Senior Management Team only.

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 "Daves". 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 the Data Protection Officer, your line manager or an individual with sufficient technological expertise.

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. Examples of third party processors include:

- sports affiliated bodies
- payroll
- website hosting.

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.

The Union has a standardised data sharing contract which may be used where the data processor does not have their own standardised format.

The GDPR places restrictions on the transfer of personal information outside of the European Economic Area (EEA) and as such no employees shall transfer data outside of this area or use non-authorised platforms that might be at risk of this without the explicit consent from the Data Protection Officer.

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 includes 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 organisations 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, please refer the requestor to the 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, including:

- 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 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 or line manager, isolating any potential for further breach where appropriate. The DPO and other involved parties should follow the below action plan
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 or line manager, isolating any potential for further breach, where appropriate. The Data Protection Officer and other involved parties should follow the below action plan.
Audit or assessment	The Union conducts termly data audits of its spaces and IT infrastructure. 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 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, the Senior Management Team must be advised and comprehensive guidance sought from the Information Commissioner's Office.	Immediately report the matter to the Data Protection Officer and a member of the Senior Management Team of the Union. The Data Protection Officer 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, 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 Data Protection Officer 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 11,000 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 to ensure procedures, policies and equipment is of sufficient security standard to avoid future breaches in this mechanism.

Disposing of data

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

- **Member data**: In line with University policy, member (student) files shall be removed from six years after a student graduates or otherwise leaves the University.
- **Employee data**: The Union will keep employment history data about former employees for 100 years from the date of birth in order to verify employment details of former staff. Most other data will be removed 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.
- **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 records will be deleted through the decommissioning of equipment by the University IS&T department and digital records shall be deleted from databases at source.

6. 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 example to process an individual's membership, and who it has been shared with. The individual needs to make the request in writing.

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
- 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 five 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
- CCTV footage
- 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

If a verbal request is received, the employee should inform the individual that they need to put their request in writing – details of the address they should contact are in privacy notice displayed at **bucksstudentsunion.org/privacy**.

Appendix

A guide to: Displaying privacy notices

At the point of data collection the Union will provide all individuals with an easily accessible processing notice or statement, free of charge and written in plain language, which will detail:

- the identity of the Union and contact details for the DPO
- the purpose and lawful basis for the processing
- any legitimate interests of the Union and the individual in the processing of the data
- any third-party recipients of the personal data
- details of transfers to countries outside of the UK and safeguards
- retention periods or criteria used to determine the retention period
- the right to lodge a complaint with the ICO and the right to object to processing
- the consequences of failure to provide, or removal of processing rights for personal data
- whether the provision of personal data is part of a statutory or contractual requirement
- the existence of automated decision making, how decisions are made and the consequences of this form of processing.

The Union has created a number of privacy statements, along with a cookies statement, for the website, along with a confidentiality statement for the Advice Centre, which must be clearly linked from any appropriate data collection form:

- Student Data Privacy Statement
- Employee Data Privacy Statement
- Clients and Suppliers Data Privacy Statement
- Consumer Data Privacy Statement
- Cookies Statement
- Advice Centre Confidentiality Statement

A guide to: Identifying lawful processing

For processing to be lawful under the GDPR, you must identify a lawful basis before you can process any personal data. It is important that you determine your lawful basis for processing personal data and document this on the Data Collection Assessment Form.

The table below identifies the lawful processing reasons, provides relevant examples and identifies any steps that must be taken to proceed with this processing method.

Lawful processing	Organisational examples	Next steps
Consent of the data subject	Opting in to receive a commercial newsletter	There are specific requirements for gaining consent - please see advice below for gaining consent
Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract	Storage of the name and address of individuals and processing of this to send/fulfil an online purchase and manage returns programme	A copy of this contract or terms and conditions is available to view on the website with the Consumer Data Privacy Statement covering the legal basis for data processing
Processing is necessary for compliance with a legal obligation	The HMRC requires the Union to provide certain information for tax purposes	A note should be made on the data collection assessment form of the legal obligation
Processing is necessary to protect the vital interests of a data subject or another person	If someone was in a medical position that their personal information needed to be released to medical practitioners to preserve life	Post releasing this data the Data Protection Officer should be advised
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	The Union does not process any data in the public interest	
Necessary for the purposes of legitimate interests pursued by the controller or a third-party, except where such interests are overridden by the interests, rights or freedoms of the data subject	Members could legitimately expect their information to be processed to enable membership focused services	A legitimate impact assessment must be completed to ensure a balance of interests is achieved. Details on how to complete this are outlined below. The completed assessment must be provided with the data collection assessment. Data collected relying on legitimate interest must declare the legitimate interest at the point of collection.

Gaining Consent

The GDPR sets an extraordinarily high standard for consent to put individuals in control, build customer trust and engagement, and enhance the organisations reputation. Consent means offering individuals genuine choice and control.

No longer can consent be assumed, there must be a positive opt-in, without pre-ticked boxes or other methods of consent by default. Explicit consent requires a very clear and specific statement of consent that's separate from other terms and conditions. If there are any third-parties that will have direct access to the data they must be specifically named and there must be a clear statement as to how to withdraw consent. This is done by a carefully curated consent statement at the point of opt in. The Data Protection Officer can help you to craft this.

In addition there is a requirement to evidence consent, the systems used to obtain content must record: who, when, how and what the individual was told.

A guide to: Processing special categories of data

There may be times when the Union processes special categories of data under the following conditions:

- explicit consent from the data subject
- carrying out obligations under employment, social security or social protection law, or a collective agreement
- protection of the vital interests of a data subject
- provided there is no disclosure to a third-party without consent (as a not-for-profit body)
- data made manifestly public by the data subject
- necessary for the establishment, exercise or defence of legal claims
- for reasons of substantial public interests
- for the purposes of preventative or occupational medicine, assessing working capacity, medical diagnosis and the provision of health or management services
- for reasons of public interest in the area of public health
- archiving purposes for statistical purposes.

A guide to: Undertaking a Legitimate Interest Assessment

A Legitimate Interest Assessment is a balancing exercise designed to test the interests of the business against the interests and rights of individuals.

As a membership organisation there are large amounts of data processing that could reasonably be carried out under this lawful processing remit - as a member individuals might legitimately expect their data to be processed in certain ways - as long as this processing does not significantly affect their rights and freedoms then this is a reasonable justification for processing of personal data.

There is a Legitimate Interest Assessment (LIA) form produced by the Union which must be completed to review the balance of interests. Having completed the form, without bias, if you feel that the individual's rights and freedoms are protected and/or there is an appropriate balance of interest towards the individual then you should proceed on the case that there is a Legitimate Interest. The LIA form can be obtained from the Data Protection Officer and once completed should be submitted to the DPO for oversight and recorded alongside the Data Collection Assessment Form.

Step one: Identify the legitimate interest

Using the tick boxes identify the legitimate interests that you believe this form of processing holds

Step two: Identify who the data is about

Using the tick boxes identify the individuals affected by this data processing

Step three: Identify if there are any special categories of data being processed

Select either 'yes' or 'no' to identify the use of special categories of data

Step four: Identify any third parties processing the data

Detail in the comment boxes any third-party data sharing - who might they be and what processes are they going to undertake with the data

Step five: Conduct a balancing test

Proceed through the questions answering either 'yes' or 'no'

Step six: Identify safeguards

In the freeform text box, detail the identified safeguards that will reduce any risk to individuals

Step seven: Review

To qualify for a legitimate interest the rights of the individual must not be outweighed by the needs of the Union in processing. Working through the balancing test section consider the individual's rights and ensure the balance leans in their favour to accept this form of legal processing. Ultimately there must be a real legitimate interest of the individual to accept this. If unsure, check with your line manager or the Data Protection Officer.

A guide to: Undertaking a Privacy Impact Assessment

A privacy impact assessment (PIA) is a tool which helps the Union identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. Employees and volunteers, supported where appropriate by the Data Protection Officer, must undertake a PIA when starting any project that handles individuals' data. This could include: new IT systems, data sharing initiatives or using existing data for new purposes.

A PIA identifies the information flow, any risks to privacy, evaluates the solutions and provides a record of the outcomes to integrate into any plan. PIA's need not be a barrier collection - the Union has a simple Privacy Impact Assessment Form which should be obtained from the Data Protection Officer and once completed submitted back to the DPO with the Data Collection Assessment Form.

Step one: Identify the need

The majority of projects will need a privacy impact assessment. However, it's worth checking that it definitely is needed. If you answer 'no' to all of the questions below you do not need to complete a PIA.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

Step two: Describe the information flows and risks

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

You will also need to explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the PIA process.

Step three: Formally identify the privacy and related risks

In the previous step you identified the risks and consulted upon them. In this step you need to take the key privacy risks identified and the associated compliance and corporate risks.

Step four: Identify privacy solutions

Now transfer these risks and describe the actions you could take to reduce them, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

Step five: Sign off and record the PIA outcomes

Review these risks with your line manager and get sign off on these. If you need to consult further advice from the Data Protection Officer now is the last opportunity as part of this process.

Step six: Integrate the PIA outcomes back into the project plan

As a privacy by design principle these risks and control measures should be built into the project that requires the data protection. Outline at this point who is responsible for implementing the solutions that have been approved and who is the contact for any privacy concerns which may arise in the future.

Data Processor Agreement for third-parties

This Agreement is made on the **[day]** of **[month] [year]**

BETWEEN

Bucks Students' Union ("the Union") whose registered address is: Queen Alexandra Road, High Wycombe, Buckinghamshire HP11 2JZ

And

[Supplier name] ("the Supplier") whose registered address is: **[supplier address]**

WHEREAS

a. The Union wishes to engage the Supplier to process Personal Data on its behalf, and

b. Each time the Supplier processes personal data on behalf of the Union the data will be processed on the terms and conditions laid out in this Agreement.

IT IS HEREBY AGREED THAT

Interpretation

The following terms:

"Data", "Data Controller", "Personal Data", "Data Processor" and "Processing" have the meanings given in Section 1(1) of the Data Protection Act 1998.

"Data Controller" means The Union.

"Duration" means the period of **[day]** of **[month] [year]** to the **[day]** of **[month] [year]** during which the data will be processed

"Personal Data" means **[list of data to be transferred]**

"Processing Activity" means **[the nature and purpose of the processing]**

"Confidential information" means The Union and the Data Controller's secrets and confidential information and extends to all knowledge or information relating to both, their organisation, finances, processes and membership information held by the Union.

Data processing

1. The terms of this Agreement shall apply for the Duration of the Processing Activity whenever the Supplier processes data on behalf of the Union.

2. The Union, as the data controller, is liable for compliance with the GDPR and 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.

3. The Supplier, as a data processor, will:

3.1. Act only on the written instructions from the Union (unless required by law to act without such instructions);

3.2. Ensure that people processing the data are subject to a duty of confidence;

3.3. Take appropriate measures to ensure the security of processing;

3.4. Only engage a sub-processor with the prior consent of the data controller and a written contract;

3.5. Assist the Union in providing subject access and allowing data subjects to exercise their rights under the GDPR;

3.6. Assist the Union in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

3.7. Delete or return all personal data to the controller as requested at the end of the contract;

3.8. Provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state; and

3.9. Ensure appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Confidentiality

4. The Supplier shall, both during this Agreement and after its termination (without limit in time), keep confidential and not use or disclose or attempt to use or disclose any confidential information supplied by the Union or its members, except as authorised or required by the purposes of this Agreement.

5. Confidential information will only be made available by the parties to those of their staff and agents who have a reasonable need to know of it. The documents or other materials and data or other information or copies thereof will not be made available to any third-parties except for professional advisers in confidence or if required by law.

6. The Supplier shall not under any circumstances subcontract the processing of the Union's data without prior written permission from the Union to do so.

7. Either party is entitled to demand the return of any documents or other material or data or other information supplied to the other party under this Agreement within one month of giving the other party written notice.

8. On the cessation or earlier termination of this Agreement, each party shall return to the other all documents or other material containing confidential information and destroy any surplus copies.

9. Paragraph 7 of this Agreement shall not apply to documents, other materials, data or other information which are already in the public domain at the time when they were provided by either party or if at any time the information becomes public knowledge through no fault of the other party.

10. Both parties undertake that any information which is received from the other party under this Agreement will only be used for the purposes of this Agreement.

Requests for information

11. The Supplier must inform the Union immediately (within two working days) of any requests it receives for copies of the Union data, and only respond to any such request as directed by the Union or the Data Controller. The Supplier shall also co-operate fully with any reasonable requests made by the Union or Data Controller in relation to any such requests.

Inspection

12. The Data Controller may, on reasonable notice and during business hours, inspect the Supplier's data processing facilities, data files and relevant documentation.

Indemnity

13. Nothing within this agreement relieves the supplier of its own direct responsibilities and liabilities under the GDPR.

14. The Supplier shall indemnify the Data Controller, against any loss or damage it sustains or incurs as a result of any loss, theft or un-repairable damage to the Union's data or any other failure by the Supplier to comply with its obligations under this Agreement, including any regulatory fine imposed on the Data Controller because of the Supplier's action or omission.

Governing law

15. This Agreement is subject to English Law and the parties submit to the non-exclusive jurisdiction of the English Courts.

Signed …….

Name……..

For and on behalf of Bucks Students' Union

Signed ……..

Name……..

For and on behalf of the Supplier

Reporting a breach flowchart