THE STUDENTS' UNION (THE SU) DATA PROTECTION POLICY

Purpose: The SU, University of Bath needs to hold and process certain personal information to effectively provide our services.

This policy describes how we collect, handle and store personal data.

Rationale: The Data Protection Act 1998 requires that organisations who collect personal data do so in a fair and lawful way. The General Data Protection Regulation (GDPR) comes in to effect May 2018 and reinforces certain principles, specifically around an individual's right to access and understand what data we hold about them and what we are doing with it.

The Information Commissioner's Office (ICO) provides independent advice and guidance about data protection and freedom of information.

Responsibilities

Everyone who works for or with The SU has some responsibility for ensuring data is collected, stored and handled appropriately.

Each staff member, student or agent directly involved in supporting SU services or activities must ensure that personal data is handled and processed in line with this policy and the ICO data protection principles.

For the remainder of this document, anyone in this position is referred to as a **'data handler'**.

The SU Employees

All staff will have access to personal data and will use the processes and platforms provided by the SU and University to ensure that data is managed securely.

They will adhere to the procedures detailed below and will support Student Leaders in their activities.

Reviewed:	18/10/2018
Next Review:	18/10/2020

Student Leaders

Our Student Leaders can communicate with their memberships through secured email lists and will be trained in the below procedures to ensure that any organisational activities (such as event organisation or tournament registration) are managed with staff support to ensure they follow data protection best practice.

Data Co-ordinator

The designated Data Co-ordinator is responsible for the documentation and processes used by The SU to meet compliance, and is there to support all data handlers with best practice.

Board of Trustees

The Board of Trustees holds ultimate accountability for The SU, delegating responsibility for the day-to-day management of the organisation to our Chief Exec.

Procedures

Data should **only be used for its intended purpose.** This purpose will be declared in our Privacy Notice or at the point when the data is collected.

Data should only be collected when needed, and **only collect that which is required**.

Personal data **should never be disclosed** to unauthorised people, either within The SU, University or externally.

Strong passwords must be used for computer and application logins and they should never be shared.

The SU will provide training to all data handlers to help them understand their responsibilities.

Data handlers **should follow the guidance provided and request help** from the Data Co-ordinator (suweb@bath.ac.uk) if they are unsure about any aspect of data protection.

Special Category Data

Certain types of information are considered more sensitive than others, the list includes:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Data of this nature must be treated with extra care; whenever this type of information needs to be collected or shared, please seek the support of the Data Co-ordinator at suweb@bath.ac.uk

Sharing data with third parties

Whatever the reasons for sharing data with third parties, in almost every circumstance the consent of each individual is needed.

Put simply, if an individual does not know that their information is going to be passed to another party, then the data must not be shared.

- Speak to the Data Co-ordinator before doing anything
- Make sure you have a record of consent from each individual in the data (see Gathering Consent section). We may already have consent for certain tasks – check with the Data Co-ordinator.
- When sending large amounts of data, or anything containing Special Category Data, password protect the file and send the password in a separate email or advise the recipient over the phone.

Exceptions to the above include the third party applications used by The SU to conduct its core business.

The risks and security of these systems have been reviewed and we have ensured that their use is fair and lawful. Details about these can be found in our Privacy Notice.

Storing and moving data

We have solutions in place for all known activity, if you think that these mechanisms cannot work for your particular task, please contact the Data Co-ordinator at **suweb@bath.ac.uk**

MSL (Our Customer Relationship Management System)

This is where student data is pre-loaded from SAMIS (details on our Privacy Notice), and will hold details of many interactions a student carries out such as ticket purchases.

You can securely download reports from this system.

University-managed storage

Can be used for storing all types of data.

Make sure **any** files containing sensitive data are in a directory with restricted administrative permissions, or the files themselves are password protected.

Line managers should store reviews and other documents about their staff on their own H drive as opposed to the general Resource drives.

University-managed cloud storage

Some cloud storage solutions may become available in the near future. This policy will be updated in due course.

University-managed email

Can be used for sending most things, but thought should be given when you need to share large amounts of personal data, or sensitive data; It is better to share a link to a location on University-managed storage if sharing internally, otherwise ensure you password protect the file and send the password in a separate email or advise the recipient over the phone.

thesubath.com

The website contains an online form tool that can be used to collect data.

If you need to collect sensitive data using this tool, please speak with the Data Co-ordinator to ensure the data is subsequently removed from MSL's servers and securely downloaded to University-managed storage.

Other engagement reports from the website can be obtained from The SU Marketing and Communications team on request.

Any file uploaded to the web interface of thesubath.com will be publicly accessible, please consider this before uploading anything to the site.

Personal computers and USB keys

Make sure any local files that contain personal data are permanently deleted from your computer.

This includes the 'Downloads' folder and the recycle bin/trash.

USB keys **should not be used** to transport personally identifiable data.

Personal email and personal cloud storage accounts

Should **never** be used!

Gathering consent

There are normally two scenarios when it comes to sharing data:

Sharing information you already have

If you need to share information that you already have about a group of individuals, it is important that you get their consent before doing so.

You could send them all an email and ask them to confirm by response (you must receive a response… inaction buy the individual does not mean they have given consent), or you could set up an online form and ask them to quickly complete it.

Either way, you will end up with a record of consent.

Sharing information you are about to request (e.g. from an online or paper form)

If you are creating a form for individuals to fill in, and that information will then be shared, make sure you put a clear statement on the form that explains what is going to happen to that data, and why.

Make sure there is a mandatory 'I agree' checkbox next to this statement if collecting online, and do not pre-tick this box.

You should also request ALL the info you need on this form – don't auto-populate any data afterwards (e.g. their date of birth or phone number, if you happen to have access to it elsewhere)

If you need to share Special Category Data (see above), please discuss with the Data Co-ordinator by emailing suweb@bath.ac.uk

Photography and filming

If taking photos or film at an event, **make sure that everyone in attendance knows you are doing so, and where that content might be used**.

This gives people the opportunity to tell the photographer not to include them, or move to a position where they will not be filmed (especially important if an event is controversial or requires a degree of sensitivity to its attendees).

Please use our Location Warning Notice template

Photos

In some cases it is more appropriate to get individual's explicit consent, examples include:

- A guest speaker or performer at an event
- Photos where a small number of people are clearly the subject *

* You may find the Location Warning Notice is enough, but if a photo is particularly good and you think it may be used on promotional material, it is better to get explicit consent from those who are the obvious focus of the picture.

Please use our Photographic Consent Form

Filming

If an individual is the specific focus of filming, you must get their consent.

Filming crowds of people at an event does not require individual consent, but make sure you used the Location Warning Notice (again, this is very important at events where the subject matter is sensitive or controversial).

Please use our Filming Consent Form

Using Social Media

Using social media accounts is perfectly fine as long as communication and information stays within the platform that is being used.

Data handlers must not copy any information about an individual for their own purposes e.g. If a person's social media profile suggests they are vegan, this is not a declaration, nor should you assume it is accurate; obtain this information directly from the individual.

Ensure that where possible, the account/page/group is linked to a University of Bath email address and not your personal account.

Don't forget that the photos you add to social media are personal data – see the Photography and filming section above.

If you receive a request from someone to remove their image from social media, please do so as soon as you can.

Information recorded on paper

The general principles mentioned in this policy apply to both electronic data and that written or printed on paper.

If you are collecting personal details on paper, make sure you read the Gathering Consent section.
Make sure anything you want to keep on paper is kept securely and is only accessible to those who are allowed.

Paperwork should be put in our confidential waste bins when it is no longer needed.

Right to access and edit personal information

Everyone who has data on our system has the right to request details of exactly what is stored and where.

They also have the right to amend the details we hold about them.

Please refer any requests of this nature to the Data Co-ordinator at **suweb@bath.ac.uk**

Objections to the processing of an individual's data and their right to be forgotten

Where appropriate, an individual can request that we cease processing of their data, or remove their information completely from our records.

Please refer any requests of this nature to the Data Co-ordinator at **suweb@bath.ac.uk**

Data breach (when data goes missing or is shared with the wrong people)

If any personally identifiable data is lost or shared outside of the boundaries of this policy, whether accidently or maliciously, **the Data Co-ordinator must be notified immediately** by emailing **suweb@bath.ac.uk**

Data accuracy and review

The Data Co-ordinator keeps an ongoing review schedule for the applications and storage solutions used by The SU and its data handlers.

This is to ensure that all data being held is being done so for legitimate reasons and that anything no longer needed is deleted.

Automated deletion and anonymisation occurs on some of our applications and is detailed in our Privacy Notice.

Data handler permissions for applications and storage access will also be regularly reviewed.

Reviewed:	18/10/2018
Next Review:	18/10/2020