South Bank Students' Union Data Protection Policy

Last updated June 2024

Introduction

1 Data Protection Policy Statement

1.1 South Bank Students Union Ltd (SBSU) is committed to the protection of individuals' rights and privacy. We will take all necessary steps to protect the personal data that we hold and will do this through effective data management and adhering to the UK General Data Protection Regulation 2018 (UK GDPR) and the Data Protection Act (2018).

1.2 This policy provides a framework to help ensure that SBSU meets its legal obligations under the legislation.

1.3 SBSU is a separate legal entity from London South Bank University (LSBU). However, SBSU is a key partner of the University and is has entered into a Data Sharing agreement with LSBU which can be read here. This policy should therefore be read alongside this document, and with reference to LSBU's Data Protection Policies and Procedures which can be found here.

1.4 SBSU is the Data Controller for collecting and using personal data and is registered with the Information Commissioner's Office (ICO) (registration number ZB291231).

2 Scope of policy

2.1 This policy covers all personal data and special categories of data (sensitive personal data) that we process about data subjects. In relation to individual rights, the policy applies to anybody about whom we hold personal and/or sensitive information.

2.2 In relation to data processing, it applies to anyone who processes personal and/or sensitive information on behalf of SBSU, including current, past and prospective staff, trustees and visitors of SBSU. We use the term 'staff' in this policy to include those working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed term employees, casual and agency staff and volunteers (including student volunteers).

3 Aims of policy

3.1 The aims of this policy are to:

3.1.1 Ensure the safe and legal processing of all personal data by SBSU (and all who handle or process data on behalf of SBSU) in accordance with the GDPR UK and Data Protection Act 2018.

3.1.2 Ensure that there are proper procedures in place for the lawful processing of personal data, and systems for the management and monitoring of those procedures.

3.1.3 Communicate to all staff, trustees and students their responsibilities relating to data protection at SBSU.

3.1.4 Assure all data subjects that their data is always secure and safe from unauthorised access, alteration use or loss.

3.1.5 Communicate to data subjects their rights relating to personal data we hold.

4 Data Protection Principles

4.1 SBSU commits to adhere to the six Data Protection Principles set out in the UK GDPR when processing personal data. These specify that personal data must be:

4.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

4.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

4.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

4.1.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

4.1.6 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.

4.2 In addition to the above principles, the UK GDPR also sets out an overarching accountability principle which is that 'the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

5 Definitions

5.1 **Data Protection Legislation** - Both the General Data Protection Regulations (2018) and the Data Protection Act 2018.

5.2 **Personal Data** - Any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier.

5.3 **Special Category Data** - Personal data relating to:

- ethnic origin,
- physical and mental health (including, for example, details of reasons for sick leave),

- sex life,
- genetics,
- biometrics (where used for ID purposes),
- religion or belief,
- political opinion,
- Trade Union membership,

Greater protections are required when processing this data.

5.4 **Processing** - Obtaining, recording, holding or adding to the information or data or carrying out any operation or set of operations on the information or data.

5.5 **Data Subject** - An individual who is the subject of the personal data.

5.6 **Data Controller** - A person who, or organisations which (either alone or jointly or in common with other persons/organisations) determines the purposes for which, and the way any personal data is processed. In this case, this means SBSU or nominated individuals acting on behalf of and with the authority of SBSU.

5.7 **Data Processor** - Any person (other than a member of staff) or organisation who processes data on behalf of SBSU.

5.8 **Data Subject Access Request** - Any data subject about whom SBSU holds or uses personal data has a legal right to access that information and request a copy of the data in permanent form.

5.9 **Data Protection Impact Assessment** - A formal assessment of the impact of processing on the individual including the risks and any impact on their rights and freedoms.

5.10 **Breach** - Any incident, or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of Personal Data.

5.11 **Privacy Statement** - A document informing the data subject of the legal basis, purposes of processing etc.

5.12 **Data Sharing Agreement** - An agreement between LSBU and SBSU which governs the sharing of personal data of data subjects which are shared by both parties.

5.13 **Information Commissioner** - The Information Commissioner oversees the implementation of Data Protection Legislation.

5.14 **Staff -** Unless otherwise applicable, all references to staff include all current, past and prospective staff working at **all** levels and grades, full-time, part-time staff including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed term employees, casual and agency staff, trustees and volunteers (including student volunteers).

5.15 **Students** - Unless otherwise applicable, all references to students include all current, past and prospective students, whether full-time or part-time.

5.16 Other definitions and terms used in relation to the GDPR (2018) can be found here.

6 Relationship with other policies, procedures and guidance

6.1 This policy should be read in conjunction with:

- SBSU Retention and Disposal of Documentation Guidelines (see Appendix F)
- LSBU Student Records Retention Schedule
- SBSU Privacy Notice
- LSBU – LSBSU Data Sharing Agreement
- LBSU IT Security Policy (For staff)

7 Roles & Responsibilities

7.1 The **Board of Trustees** - The Board of Trustees has a duty to ensure, so far as is reasonably practicable, that SBSU protects personal information that the organisation holds about staff, students and visitors. The Board of Trustees has a key collective role in providing leadership in relation to data protection issues, receiving reporting on data protection performance and being notified of any major incidents.

7.2 **Delegated responsibilities**:

7.2.1 **Data Protection Officer (DPO**) - The Board of Trustees has delegated the day-to-day responsibility for data protection compliance to the Chief Executive, who has been nominated as the Data Protection Officer (DPO) for SBSU.

7.2.2 The **Chief Executive** has overall responsibility for data protection and the implementation of this policy. They, and those acting on their behalf, will have responsibility for:

- ensuring that the policy is effectively implemented and reviewed so there is statutory compliance at all times;
- providing adequate resources for the provision of data protection systems and procedures;
- nominating competent persons to provide assistance on data protection and seeking external advice where necessary.

7.2.3 Specifically, the DPO will undertake the following:

- manage the coordination and implementation of SBSU's statutory responsibilities in relation to data protection according to the principles and individual rights set out in this policy;
- ensure that appropriate systems are in place to enable the fair collection, processing, safeguarding and retention/deletion of personal data in compliance with the UK GDPR;
- establish effective communication with LSBU and ensure that the LSBU – LSBSU Student Union Data Sharing Agreement is implemented;
- ensure data is kept secure in compliance with relevant LSBU and SBSU IT security policies;
- coordinate the ongoing recording of the lawful bases for processing data via a data information audit;
- act as the first point of contact for supervisory authorities and for individuals whose data is processed; this includes coordinating responses to Subject Access Requests, requests for deletion, restriction and rectification of data, and objections and complaints;
- ensure that staff, students and visitors know and accept their responsibilities regarding data protection and have the necessary information, supervision and training to enable them to competently process personal information;
- communicate how this policy, and related policies and procedures including the Privacy Policy and appendices to this policy, affect staff and data subjects, and communicate any changes to the policy;
- set up reporting, record-keeping, monitoring and review systems, aimed at continuous improvement of data processing;
- assess the impact of new information SBSU intends to collect, and arrange for a Data Protection Impact Assessment to be conducted if necessary;
- coordinate an annual data cleanse to ensure retention schedules are adhered to;
- report any serious data breaches to the ICO within 72 hours of becoming aware of the breach, and where the breach is related to shared personal data, to LSBU within one working day;
- communicate lessons learnt during the investigation of breaches to relevant parties to enable necessary improvements to be made;

- maintain SBSU's registration with the ICO;
- oversee data sharing agreements between SBSU and third parties, where there is a valid business reason for sharing information, and issue data sharing guidance;
- report to the Board of Trustees on data protection performance and management via the annual Compliance Management Plan;
- advise the Board of Trustees on its statutory obligations including relevant legislative changes.

7.2.4 **Line managers** - Line managers have a responsibility to:

- ensure that staff they line manage have read and understood this policy, and attend mandatory induction data protection training within the agreed timeframe;
- as part of the staff appraisal process, identify any data protection training needs;
- ensure that staff under their management process personal data in line with the requirements of the UK GDPR;
- ensure that members of staff will have access to personal data only where it is required as part of their functional remit;
- immediately report any data breaches brought to their attention by staff to the DPO.

7.2.5 **All staff** - All staff are responsible for complying with data protection principles and observing individuals' data protection rights. Staff must:

- read and familiarise themselves with the whole of the Data Protection Policy document;
- follow procedures as advised by the Data Protection Officer and outlined in this and other relevant policies in relation to data processing;
- complete compulsory data protection training as required and raise any personal concerns about capacity or capability in data management with line manager;
- advise the Data Protection Officer in the event of any intended new purposes for processing personal data;
- regularly review the records they keep in the course of their duties to ensure that the documents they hold are within the relevant destruction time limits set out in Appendix F;

- update their employee records and payroll information through digital employee record system of SBUS's People team;
- immediately report any actual, near miss, or suspected data breaches to the DPO for investigation;
- not attempt to gain access to information that is not necessary to hold, know or process.

7.2.6 Note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct. It may also result in a personal liability for the staff member as there is provision within the legislation to prosecute individuals for certain offences.

8 Individual rights

8.1 SBSU will respect individuals' rights when processing personal data. These are set out in GDPR (2018) as:

8.1.1 The right to be informed - we will inform you if we are using or storing your personal information;

8.1.2 The right of access - you can ask us for a copy of your personal information by making a subject access request;

8.1.3 The right to rectification - if you think the personal information we hold about you is not right you can ask us to correct it;

8.1.4 The right to erasure - you can ask us to delete your information and, if we are able to, we will do so;

8.1.5 The right to restrict processing - you may want to stop us from using your information for some purposes;

8.1.6 The right to data portability - as well as being able to ask for a copy of your information you can ask for it to be in a format that makes it accessible if you wish to share it with others. SBSU has the right to refuse a request to share your date on the basis that it is excessive or unfounded in line with ICO guidance;

8.1.7 The right to object - if you are concerned about how we are using your information you can tell us;

8.1.8 Rights in relation to automated decision making and profiling - if you think that we have made a decision about you automatically, for example by a

machine or computer, you can ask for the decision to be reviewed by a living person.

8.2 The rights above depend upon the lawful basis for processing. For example, the right to erasure only applies where the lawful basis for processing is consent. Where public task, legitimate interests, contractual basis or a legal requirement are used as the basis for processing, the right of rectification, restriction and the right to object are also limited to ensuring that the data is accurate before it can be processed.

8.3 The right to be informed is, however, a key right and applies in all circumstances.

8.4 How to exercise your rights: SBSU is committed to empowering you to understand your rights when it comes to the data we hold about you. If you have any questions, issues or concerns, please contact the Data Protection Officer by email at data-protection@lsbsu.org.

8.5 There are forms on the SBSU website and in the appendices which you can use to contact the Data Protection Officer to:

- ask for a copy of your personal information (Subject Access Request)
- ask us to delete, rectify and/or restrict the information we hold about you
- complain about how we are holding your personal information

8.6 Subject Access Requests (SARs) will be responded to and disclosure of information (subject to exemptions) provided within one calendar month. SBSU will not charge a fee to process SARs, but we reserve the right to charge an administration fee if the request is excessive, repetitive, or for additional copies of previously provided data.

8.7 If a fee is applied to your request, we will notify you in advance. The 30-day response period will pause until payment is received and will resume once paid.

8.8 Personal information will not be disclosed without proof of identity. Third party personal data will not be released when responding to SARs, unless consent is specifically obtained, obliged to be released by law or necessary in the substantial public interest.

9 How to report a data breach

9.1 If something goes wrong and you know or suspect that there has been a personal data breach and personal information has not been adequately protected, please let us know immediately by emailing data-protection@lsbsu.org.

9.2 If you are an SBSU employee, please also notify your line manager.

9.3 In some instances, we may need to report the personal data breach to the ICO, which we will do within 72 hours of us becoming aware of the breach.

9.4 If a data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those individuals without undue delay.

10 Reviewing

10.1 The Data Protection Officer is responsible for ensuring that the Data Protection Policy is up-to-date and will notify the Board of Trustees when the policy needs revision.

10.2 This assessment will be made annually or if there is legislative change or other changes in circumstances (e.g., a change in responsibilities or personnel).

11 Whistleblowing

11.1 If a member of staff has concern about a dangerous or illegal activity or any wrongdoing within SBSU, they can seek advice about whistleblowing from Protect's free and confidential advice line: 020 3117 2520.

11.2 Such concerns can include believing that your concerns won't be dealt with properly or may be covered up, that you have raised a concern, but it hasn't been acted upon, or that you're worried about being treated unfairly.

11.3 SBSU is committed to ensuring that staff and volunteers who in good faith whistleblowing in the public interest will be protected from reprisals and victimisation.

Appendices

A Lawful basis for processing

SBSU must determine the lawful basis for processing before starting any collection of personal data. The lawful bases for processing are set out in Article 6 of the GDPR and at least one of these must apply whenever personal data is processed:

a. **Consent:** the individual has given clear consent to process their personal data for a specific purpose;

b. **Contract:** the processing is necessary for a contract with the individual, or because they have asked SBSU to take specific steps before entering into a contract;

c. **Legal obligation:** the processing is necessary to comply with the law (not including contractual obligations);

d. **Vital interests:** the processing is necessary to protect someone's life;

e. **Public task:** the processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law;

f. **Legitimate interests:** the processing is necessary for the SBSU's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

In addition to having one of the lawful bases outlined above, the processing must also be necessary.

To process special categories data, SBSU must also ensure that one of the following applies:

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection;

c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. processing relates to personal data which are manifestly made public by the data subject;

e. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

f. processing is necessary for reasons of substantial public interest, on the basis of EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

g. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or UK law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph;

h. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or UK law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

i. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Once SBSU has determined the lawful basis for processing, this will be documented in the data records for each form of processing.

SBSU Subject Access Request Form

The General Data Protection Regulations (GDPR) provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to see your data. You will also need to provide proof of your identity. Your request will be processed and responded to within 30 calendar days upon receipt of a fully completed form and proof of identity.

Proof of identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of two documents such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The documents should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Administration fee

There is no fee for Subject Access Requests. However, we may charge a reasonable fee if a request is excessive, repetitive, or for additional copies of previously provided data.

If a fee applies, we will notify you in advance. The 30-day response period will pause until payment is received and will resume once paid.

Section 1: Data Subject

Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	Mr [ ] Mrs [ ] Ms [ ] Miss [ ] Other [ ]
Surname/Last Name	
First Name(s)	

Date of Birth	
Address	
Post Code	
Email Address	
Day Time Telephone Number(s)	

Identification

I am enclosing the following copies as proof of identity:

Birth Certificate		Driving Licence		Passport		Official letter to my address	

Personal Information Please give further details of your request here, including: • the dates your request covers • if you only wish to know about the information held in specific records • any other information that might help us with this request
Details

Employment Records If you are now or have been employed by South Bank Students' Union and are seeking personal information in relation to your employment please provide details of your Department, Role, Line Manager and Dates of Employment.
Details

Section 2: Representation

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	Mr [ ] Mrs [ ] Ms [ ] Miss [ ] Other [ ]
Surname/Last Name	
First Name(s)	

Date of Birth	
Address	
Email Address	
Post Code	
Day Time Telephone Number(s)	

Identification

I am enclosing the following copies as proof of identity:

Birth Certificate		Driving Licence		Passport		Official letter to my address	

Relationship to the data subject Please describe below your relationship to the data subject (e.g., parent, carer, legal representative):
Authorisation I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject: [ ] Letter of authority

[ ] Lasting or enduring power of attorney

[ ] Evidence of parental responsibility

[ ] Other _____

Section 3: Declarations

Data Subject Declaration

I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that South Bank Students' Union is obliged to confirm proof of identity/authority, and it may be necessary to obtain further information to comply with this subject access request.

Name	
Signature	
Date	

OR *(if applicable)*

Authorised Declaration

I confirm that I am legally authorised to act on behalf of the data subject. I understand that SBSU is obliged to confirm proof of identity/authority and it may be necessary to obtain further information to comply with this subject access request.

Name	
Signature	

Date	

Warning: a person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution.

Section 4: Actions

I wish to:

[ ] Receive the information in electronic format

[ ] Receive the information by post*

[ ] Collect the information in person

[ ] View a copy of the information only

[ ] Go through the information with a member of staff

**Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.*

Please complete this form electronically and email it, with scans of your proof of identity, to: data-protection@lsbsu.org.

Alternatively, you can post your completed form and proof of identity to:

Data Protection Officer
South Bank Students' Union Ltd
103 Borough Road
London
SE1 0AA

SBSU Data Rectification Form

The General Data Protection Regulations (GDPR) provides you, the data subject, with a right to rectify any data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to rectify your data. You may also need to provide proof of your identity. Your request will be processed and responded to within 30 calendar days upon receipt of a fully completed form and proof of identity (where required).

Proof of identity

We may require proof of your identity before we can amend personal data. The data protection officer will advise if proof of identity is required. If you have changed your name, please supply relevant documents evidencing the change.

> **Please note:** If you are a student at South Bank University and a member of the Students' Union, your data updates, usually nightly, with any amendments you have made to your student registry file after they have been enacted by the University. This system is a one-way system, and will over-write data that we hold about you, even if you have rectified it. Please ensure if you are changing information such as your surname, you do it first with the University, wait until that process completes, and then with us.

Administration fee

Requests to correct inaccurate or incomplete personal data are generally processed free of charge. However, if a request is manifestly unfounded or excessive, particularly if it is repetitive, we may charge a reasonable administrative fee to cover processing costs.

If a fee applies, we will notify you in advance. The 30-day response period will pause until payment is received and will resume once paid.

Section 1: Data Subject

Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	Mr [ ] Mrs [ ] Ms [ ] Miss [ ] Other [ ]

Surname/Last Name	
First Name(s)	
Date of Birth	
Address	
Post Code	
Email Address	
Day Time Telephone Number(s)	

Rectification Request Please detail in the box below, with as much information as possible, the data/information that you wish to be rectified.
Details

Reason for rectification South Bank Students' Union will not unreasonably prevent rectification of data however requires an appropriate reason to make such amendments. Please detail below the reason for requiring the data rectification.
Details

Section 2: Representation

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity (as well as that of the data subject if required by the Data Protection Officer) and proof of your right to act on their behalf.

Title	Mr [ ] Mrs [ ] Ms [ ] Miss [ ] Other [ ]

Surname/Last Name	
First Name(s)	
Date of Birth	
Address	
Email Address	
Post Code	
Day Time Telephone Number (s)	

Identification

I am enclosing the following copies as proof of identity:

Birth Certificate		Driving Licence		Passport		Official letter to my address	

Relationship to the data subject

Please describe below your relationship to the data subject (e.g., parent, carer, legal representative):

Authorisation

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

[ ] Letter of authority

[ ] Lasting or enduring power of attorney

[ ] Evidence of parental responsibility

[ ] Other _____

Section 3: Declarations

Data Subject Declaration

I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that South Bank Students' Union is obliged to confirm proof of identity/authority, and it may be necessary to obtain further information to comply with this subject access request.

Name	
Signature	
Date	

OR *(if applicable)*

Authorised Declaration

I confirm that I am legally authorised to act on behalf of the data subject. I understand that SBSU is obliged to confirm proof of identity/authority, and it may be necessary to obtain further information to comply with this subject access request.

Name	
Signature	
Date	

Warning: a person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution.

Section 4: Actions

Please complete this form electronically and email it to: data-protection@lsbsu.org.

Alternatively, you can post your completed form and proof of identity to:
Data Protection Officer
South Bank Students' Union Ltd
103 Borough Road
London
SE1 0AA

SBSU Data Erasure Form

The General Data Protection Regulations (GDPR) provides you, the data subject, with a right to erasure of any data/information we hold about you (also known as the right to be forgotten) or to authorise someone to act on your behalf. Please complete this form if you wish to rectify your data. You may also need to provide proof of your identity. Your request will be processed and responded to within 30 calendar days upon receipt of a fully completed form and proof of identity.

Proof of identity

In certain circumstances we may require proof of your identity before we can amend personal data. The Data Protection Officer will advise if proof of identity is required. If you have changed your name, please supply relevant documents evidencing the change.

Administration fee

SBSU's policy is not to charge for rectification requests. However, if a request is manifestly unfounded or excessive, particularly if it is repetitive, we may charge a reasonable administrative fee to cover processing costs.

If a fee applies, we will notify you in advance. The 30-day response period will pause until payment is received and will resume once paid.

Section 1: Data Subject

Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	Mr [ ] Mrs [ ] Ms [ ] Miss [ ] Other [ ]
Surname/Last Name	
First Name(s)	
Date of Birth	

Address	
Post Code	
Email Address	
Day Time Telephone Number(s)	

Identification

I am enclosing the following copies as proof of identity:

Birth Certificate		Driving Licence		Passport		Official letter to my address	

Data Erasure Choice

You may choose to have some, or all, of the data that we about you hold erased. You need to be aware that by choosing to erase data that South Bank Students' Union holds we may be forced to restrict services as we are required to process certain data to deliver these services.

[ ] Tick this box for ***full data erasure*** and agree to the statement below:

I would like to request a full erasure of all data that South Bank Students' Union (SBSU) holds about me. I understand that full erasure will result in the complete revocation of Students' Union membership and access to facilities and services. In addition, I agree that SBSU may retain a record of my Student ID number issued by London Southbank University to ensure that SBSU does not process any data linked with this record. Further, I agree to SBSU informing London South Bank University, who supply core information to SBSU to facilitate our membership, that I have by default chosen to opt-out of membership of SBSU.

[ ] Tick this box for ***partial data erasure*** and agree to the statement below:

I would like to request a partial erasure of all data that South Bank Students' Union (SBSU) holds about me. I understand that this erasure may result in the partial or complete revocation of LSBU membership, and access to facilities and services. The Data Protection Officer will advise of loss of service prior to erasure. In addition, I agree that SBSU may retain a record of my Student ID number issued by London South Bank University and to ensure that SBSU does not process any data linked with this record. Further, I agree to SBSU informing London South Bank University, who supply core information to SBSU to facilitate our membership, that if through my partial erasure of data, my membership of the SBSU can no longer be facilitated, that I have opt-ed out in order that no further data about me is shared between LSBU and SBSU.

Please detail below the data that you wish to be partially erased:

Identification of data

Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details

Reason for erasure South Bank Students' Union will not unreasonably prevent erasure of data however requires an appropriate reason to make such amendments. Please detail below the reason for requiring the data erasure.
Details

Section 2: Representation

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	Mr [ ] Mrs [ ] Ms [ ] Miss [ ] Other [ ]
Surname/Last Name	
First Name(s)	
Date of Birth	

Address	
Email Address	
Post Code	
Day Time Telephone Number (s)	

Identification

I am enclosing the following copies as proof of identity:

Birth Certificate		Driving Licence		Passport		Official letter to my address	

Relationship to the data subject

Please describe below your relationship to the data subject (e.g., parent, carer, legal representative):

Authorisation

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

[ ] Letter of authority

[ ] Lasting or enduring power of attorney

[ ] Evidence of parental responsibility

[ ] Other _____

Section 3: Declarations

Data Subject Declaration

I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that South Bank Students' Union is obliged to confirm proof of identity/authority, and it may be necessary to obtain further information to comply with this subject access request.

Name	
Signature	
Date	

OR *(if applicable)*

Authorised Declaration

I confirm that I am legally authorised to act on behalf of the data subject. I understand that SBSU is obliged to confirm proof of identity/authority, and it may be necessary to obtain further information to comply with this subject access request.

Name	
Signature	
Date	

Warning: a person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution.

Section 4: Actions

Please complete this form electronically and email it to: data-protection@lsbsu.org.

Alternatively, you can post your completed form and proof of identity to:

Data Protection Officer
South Bank Students' Union Ltd
103 Borough Road
London
SE1 0AA

SBSU Data Restriction and Objection Request

The General Data Protection Regulations (GDPR) provides you, the data subject, with a right to object to, and restrict, the processing of any data/information we hold about you (also known as the right to be forgotten) or to authorise someone to act on your behalf. Please complete this form if you wish to rectify your data. You may also need to provide proof of your identity. Your request will be processed and responded to within 30 calendar days receipt of a fully completed form and proof of identity.

Proof of identity

In certain circumstances we may require proof of your identity before we can amend personal data. The data protection officer will advise if proof of identity is required. If you have changed your name, please supply relevant documents evidencing the change.

Administration fee

SBSU's policy is not to charge for restriction and objection requests. However, if a request is manifestly unfounded or excessive, particularly if it is repetitive, we may charge a reasonable administrative fee to cover processing costs.

If a fee applies, we will notify you in advance. The 30-day response period will pause until payment is received and will resume once paid.

Section 1: Data Subject

Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	Mr [ ] Mrs [ ] Ms [ ] Miss [ ] Other [ ]
Surname/Last Name	
First Name(s)	

Date of Birth	
Address	
Post Code	
Email Address	
Day Time Telephone Number(s)	

Processing Objection

Please give further details of the objection here, including:

- if you know in which capacity the information is being held
- any names or dates you may have; if you do not know exact dates, please give the year(s) that you think may be relevant.

Data details

Detail of objection

Processing Restrictions Please give further details of your processing restriction request here, including: • if you know in which capacity the information is being held • any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.
Data details **Detail of restriction request**
Reason for objection or restriction

South Bank Students' Union will not unreasonably prevent restriction or objection to the processing of data, however, requires an appropriate reason to make such amendments. Please detail below the reason for requiring the data rectification.
Details

Section 2: Representation

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	Mr [ ] Mrs [ ] Ms [ ] Miss [ ] Other [ ]
Surname/Last Name	
First Name(s)	
Date of Birth	
Address	
Email Address	

Post Code	
Day Time Telephone Number (s)	

Identification

I am enclosing the following copies as proof of identity:

Birth Certificate		Driving Licence		Passport		Official letter to my address	

Relationship to the data subject

Please describe below your relationship to the data subject (e.g., parent, carer, legal representative):

Authorisation

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

[ ] Letter of authority

[ ] Lasting or enduring power of attorney

[ ] Evidence of parental responsibility

[ ] Other _____

Section 3: Declarations

Data Subject Declaration

I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that South Bank Students' Union is obliged to confirm proof of identity/authority, and it may be necessary to obtain further information to comply with this subject access request.

Name	
Signature	
Date	

OR *(if applicable)*

Authorised Declaration

I confirm that I am legally authorised to act on behalf of the data subject. I understand that SBSU is obliged to confirm proof of identity/authority, and it may be necessary to obtain further information to comply with this subject access request.

Name	
Signature	
Date	

Warning: a person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution.

Section 4: Actions

Please complete this form electronically and email it to: data-protection@lsbsu.org.

Alternatively, you can post your completed form and proof of identity to:

Data Protection Officer
South Bank Students' Union Ltd
103 Borough Road
London
SE1 0AA

F Retention and disposal of documentation guidelines

1 Examples of documents which may be destroyed once they have been used or have become out of date

- Announcements and notices of meetings and other events, notifications of acceptance or apologies
- Requests for information such as maps, travel directions, brochures etc.
- Requests for, and confirmations of, reservations for internal services (e.g., meeting rooms, car parking spaces etc) where no internal charges are made
- Requests for, and confirmations of, reservations with third parties (e.g., travel, hotel accommodation, restaurants) when invoices have been received
- Transmission documents, letters, fax cover sheets, email messages, routing slips, compliment slips and similar items which accompany documents but do not add any value to them
- Message slips
- Superseded address lists, distribution lists etc
- Duplicate documents such as cc and FYI copies, unaltered drafts, snapshot printouts or extracts from databases
- Day files (chronological copies of correspondence)
- Personal diaries and address books etc
- Working papers where the results have been written into an official document, and which are not required to support it
- Stocks of in-house publications which are obsolete, superseded or otherwise useless e.g., magazines
- Published or referenced materials received from other parts of the institution or from sellers or other external organisations which require no action and are not needed for record purposes e.g., trade magazines, vendor catalogues, flyers, newsletters.

2 Document Retention

a. Staff Data - Staff data refers to any data held on permanent staff, Sabbatical Officers, and student and temporary staff collected and held in their capacity as staff.

Type of Data	Suggested retention period	Reason
Personnel files, including health records, risk assessments and appraisals	Six years from the end of employment	Reasonable period within which to provide references / CIPD advice
Pension details	12 years after benefit ceases	CIPD advice
Application forms	12 months	Equality Act 2010
References	12 months	CIPD advice
Redundancy facts	Six years from date of redundancy	Litigation
Safeguarding concerns about the behaviour of a staff member or volunteer around children	Until they reach normal pension age or for 10 years – whichever is longer Allegations found to be false should be destroyed immediately See exceptions in Guidance	NSPCC Guidance - Child Protection Records Retention and Storage Guidelines (September 2023)
Flexible working requests	18 months following any appeal	CIPD advice
Statutory sick pay	Six months after the end of period of sick leave	The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55)

Type of Data	Suggested retention period	Reason
Working time records including overtime, annual holiday, time off for dependents, etc	Two years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833)
Disciplinary records	Six years	CIPD advice
Whistleblowing documents	Six months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately.	Public Interest Disclosure 1998
Income tax and NI	Three years from the end of the financial year to which they relate	Income Tax [Employment] Regulations 1993
Maternity pay and records (including Mat B1s and shared parental, paternity and adoption pay records)		Statutory Maternity Pay [General] Regulations 1986 and Maternity & Parental Leave Regulations 1999
Personal injury claims		Limitation Act 1980
Wages and salaries	Six years	Taxes Management Act 1970
Accident books	Three years after date of last entry	RIDDOR 1995 (or until a young person reaches the age of 21)
	Removed from file after the length of time determined at disciplinary hearing	Management of employment relationship
	Three years from the date of each entry	Litigation

b. **Student Data** - All students' personal data shared by LSBU must be retained and deleted in compliance with the LSBU Student Records Retention Schedule.

Type of data	Suggested retention period	Reason
Student disciplinary records	Six years after last action on case	Possible litigation
Student advice records	Kept as long as is necessary to open and process a case and for five years from case closure	Necessary for processing and potential follow-on queries
Membership forms and related documentation (clubs, societies)	Six years after end of membership	Possible litigation Inspection (insurance)
Student data relating to the administration of elections	One year after the Returning Officer declares the final election result	Possible litigation
Student data relating to the purposes set out in Section 4.1 of the Data Sharing Agreement between LSBU and SBSU	Destroyed when the student ceases to be a LSBU student	Not required after completion of course
Student data relating to SBSU's communication with LSBU students	Destroyed when the student ceases to be a LSBU student	Not required after completion of course
Records relating to children and young adults	Until the child/young adult reaches the age of 21.	Limitation Act 1980
Safeguarding records for under-18s	Kept until the child is 25	NSPCC Guidance - Child Protection Records Retention and Storage Guidelines (September 2023)

c. Board minutes, committee and sub-group papers

Type of data	Suggested retention period	Reason
Trustee Board & Sub-Committee minutes (Leadership Team and Scrutiny Panel)	Permanent	Best practice
Trustee Board & Sub-Committee agendas and papers	Seven years	LSBU inspection, LSBU best practice, and litigation

d. Agreements and related correspondence

Type of data	Suggested retention period	Reason
Major agreements of historical significance (including, but not limited to documents from company/charitable incorporation, resolutions, memorandums and articles)	Permanent	
Contracts with customers, suppliers or agents Financial Memorandums and Block Grant Letters between LSBU and SBSU Licensing agreements Rental/hire purchase agreements	Six years after expiry or termination of the contract	Six years is generally the time limit within which proceedings founded on a contract may be brought – Section 5 Limitation Act 1980.

Type of data	Suggested retention period	Reason
Indemnities and guarantees		If the contract is executed as a deed, the limitation period is twelve years
Other agreements/contracts		Actions for latent damage may be brought up to fifteen years after the damage occurs
Property		
Leases	Memorandum and Block Grant Letter	
Procurement and related documents		
Unsuccessful tenders – documentations and quotes	Two years after the contract starts	Best practise
Documentation relating to successful tenders not covered elsewhere in these guidelines	Six years after the contract ends	See above – contract section

e. Accounts and other financial documentation

Type of data	Suggested retention period	Reason
Accounts		
Final SBSU Accounts	Permanent	Taxes Management Act 1970
Tax		

Type of data	Suggested retention period	Reason
Supporting documentation for tax returns: VAT	Six years	In general, where there is an enquiry into a tax return, records should be retained until the enquiry is complete
PAYE	For PAYE records not required to be sent to the Inland Revenue, not less than three years after the end of the tax year to which they relate	Income Tax (PAYE) Regulation 2003, Reg.97. Note however that payroll records should be kept for six years
Banking Records		
Cheques, bills of exchange, and other negotiable instruments, bank statements	Six years after end of financial year	Limitation Act 1980
Instructions to banks	Six years after ceasing to be effective	Limitation Act 1980
Printouts from accounting records for financial management purposes	Two years	Best practise
Original finance records such as invoices, credit card slips, till rolls etc	Six years following the accounting year in which they were created	Possible litigation/HMRC
Pensions		
Pension scheme documents	Permanent	CIPD advice
Furlough scheme		
Coronavirus furlough records	Six years for furlough records including amounts claimed, claim period per employee, reference	See: former statutory guidance 'Claim for wages

Type of data	Suggested retention period	Reason
	number and calculations. For flexible furlough - usual and actual hours worked.	through the Coronavirus Job Retention Scheme'.

f. Health and Safety records

Type of data	Suggested retention period	Reason
Fire warden training	Six years after employment	Fire Precautions (Workplace) Regulations 1997.
First aid training	Six years after employment	Health and Safety (First Aid) Regulations 1981.
Health and Safety representatives and employees' training	Five years after employment.	Health and Safety (Consultation) Regulations 1996; Health and Safety Information for Employees Regulations 1989
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676).

Type of data	Suggested retention period	Reason
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).
Medical records under the Control of Asbestos at Work Regulations	40 years from the date of the last entry (medical records); 4 years from the date of issue (medical examination certificates).	The Control of Asbestos at Work Regulations in 2002, 2006 and 2012 (SI 2002/ 2675) (SI 2006/2739) and (SI 2012/632).
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years.	The Ionising Radiations Regulations 1999 (SI 1999/3232).
Records of tests and examinations of control systems and protective equipment	Five years from the date on which the tests were carried out.	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).
Assessments under health and safety regulations and safety representatives and committee records (including previous COVID-19 risk assessments).	Permanently	CIPD advice

g. Employee financial records

Type of data	Suggested retention period	Reason

Payrolls/wages/expenses/overtime records	Six years from the end of the tax year to which they relate	Taxes Management Act 1970
Record of payment of employee expenses	Seven years	Taxes Management Act 1970
National Minimum Wage records	Six years after end of pay reference period following the one that the records cover	National Minimum Wage Act 1998

h. Insurance

Type of data	Suggested retention period	Reason
Policies	Six years after lapse	Limitation Act 1980 In case of litigation which may be brought within three years of the incident
Claims correspondence	Three years after settlement	
Accident reports and relevant correspondence	Three years after settlement	
Employer's liability insurance certificate	40 years	Employers' Liability (Compulsory Insurance) Regulations 1998

i. General Data

Type of data	Suggested retention period	Reason
Professional Advice Records e.g., Advice Service	Kept as long as is necessary to open and process a case and for five years after case closure	Necessary for processing and potential follow-on queries

Type of data	Suggested retention period	Reason
CCTV footage	Referred to LSBU policy	See LSBU policy
Business planning and development papers	Two years	Reference
Senior Management Team, Compliance Group, and People & Culture Group papers and minutes	Six years	Reference and litigation
Official publications of the Union	Six years	Best practise and possible litigation
Subject Access Requests	One year after last communication	Data Protection Act 2018 / CIPD advice

If you wish to retain personal data other than in accordance with these guidelines, seek guidance from SBSU's Data Protection Officer.

The Data Protection Act 1998 specifies that we should not keep personal data for longer than is necessary for our stated purposes. The above guidelines are designed to help achieve this. Equally, data subjects have the right to expect us to keep records for these necessary periods in case they should require access to them. Once the document has been kept for the maximum time it should be destroyed, with the same care taken to avoid accidental disclosure of the information. Where practicable, shredding is recommended as the most appropriate and secure way of destroying paper documents.

It should be noted that where any documents are required for investigation by relevant external bodies, they may be kept longer than indicated in the above guidelines.

GDPR Data Processing Agreement

Name of Data Controller:	South Bank Students' Union
Name of Processor:	[insert name of processor]
Date Implemented:	[insert date of agreement]
Responsibility:	[insert role here]

SBSU Data Protection Policy
June 2024

1 **THIS AGREEMENT** is made on [insert date].

BETWEEN:

1.1 South Bank Students' Union Ltd., a company registered in United Kingdom under number 13353590 whose registered office is at Student Centre South Bank University, 103 Borough Road, London, United Kingdom, SE1 0AA ("Data Controller")

and

1.2 [insert name of data processor], a company registered in [insert country of registration] under number [insert company registration number] whose registered office is at [insert registered address] ("Data Processor").

This contract is made with reference to the following facts:

1.3 Under a written agreement between the Data Controller and the Data Processor ("the Service Agreement"), the Data Processor provides to the Data Controller the Services described in Schedule 1.

1.4 The provision of the Services by the Data Processor involves it in processing the Personal Data described in Schedule 2 on behalf of the Data Controller.

1.5 Under EU Regulation 2016/679 General Data Protection Regulation ("the GDPR") (Article 28, paragraph 3), the Data Controller is required to put in place an agreement in writing between the Data Controller and any organisation which processes personal data on its behalf governing the processing of that data.

1.6 The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the GDPR in relation to all processing of the Personal Data by the Data Processor for the Data Controller.

1.7 The Data Processor will be issued with copies of the Data Controller's Data Protection and Information Security policies and agrees to adhere to these in relation to all processing of the Personal Data for the Data Controller.

1.8 The terms of this Agreement are to apply to all processing of Personal Data carried out for the Data Controller by the Data Processor and to all Personal Data held by the Data Processor in relation to all such processing.

2 **IT IS AGREED** as follows:

2.1 **Definitions and Interpretation**

In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

Data Controller, Data Processor, processing, and data subject	shall have the meanings given to the terms "controller", "processor", "processing", and "data subject" respectively in Article 4 of the GDPR;
ICO	means the UK's supervisory authority, the Information Commissioner's Office;
Personal Data	means all such "personal data", as defined in Article 4 of the GDPR, as is, or is to be, processed by the Data Processor on behalf of the Data Controller, as described in Schedule 2;
Services	means those services described in Schedule 1 which are provided by the Data Processor to the Data Controller and which the Data Controller uses for the purpose described in Schedule 1;
Sub-Processor	means a sub-processor appointed by the Data Processor to process the Personal Data; and
Sub-Processing Agreement	means an agreement between the Data Processor and a Sub-Processor governing the Personal Data processing carried out by the Sub-Processor, as described in Clause 10.

2.2 Unless the context otherwise requires, each reference in this Agreement to:

- "writing", and any cognate expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;
- a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;
- "this Agreement" is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

- a Schedule is a schedule to this Agreement; and
- a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule;
- a "Party" or the "Parties" refer to the parties to this Agreement;
- The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement;
- Words imparting the singular number shall include the plural and vice versa;
- References to any gender shall include all other genders;
- References to persons shall include corporations.

3 Scope and Application of this Agreement

3.1 The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 2, carried out for the Data Controller by the Data Processor, and to all Personal Data held by the Data Processor in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.

3.2 The provisions of this Agreement supersede any other arrangement, understanding, or agreement made between the Parties at any time relating to the Personal Data.

3.3 This Agreement shall continue in full force and effect for so long as the Data Processor is processing Personal Data on behalf of the Data Controller, and thereafter as provided in Clause 9.

4 Provision of the Services and Processing Personal Data

4.1 The Data Processor is only to carry out the Services, and only to process the Personal Data received from the Data Controller:

4.1.1 for the purposes of those Services and not for any other purpose;

4.1.2 to the extent and in such a manner as is necessary for those purposes; and

4.1.3 strictly in accordance with the express written authorisation and instructions of the Data Controller (which may be specific instructions or

instructions of a general nature or as otherwise notified by the Data Controller to the Data Processor).

5 Data Protection Compliance

5.1 All instructions given by the Data Controller to the Data Processor shall be made in writing and shall at all times be in compliance with the GDPR and other applicable laws. The Data Processor shall act only on such written instructions from the Data Controller unless the Data Processor is required by law to do otherwise (as per Article 29 of the GDPR).

5.2 The Data Processor shall promptly comply with any request from the Data Controller requiring the Data Processor to amend, transfer, delete, or otherwise dispose of the Personal Data.

5.3 The Data Processor shall transfer all Personal Data to the Data Controller on the Data Controller's request in the formats, at the times, and in compliance with the Data Controller's written instructions.

5.4 Both Parties shall comply at all times with the GDPR and other applicable laws and shall not perform their obligations under this Agreement or any other agreement or arrangement between themselves in such way as to cause either Party to breach any of its applicable obligations under the GDPR.

5.5 The Data Controller hereby warrants, represents, and undertakes that the Personal Data shall comply with the GDPR in all respects including, but not limited to, its collection, holding, and processing.

5.6 The Data Processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with any and all applicable legislation from time to time in force (including, but not limited to, the GDPR) and any best practice guidance issued by the ICO.

5.7 The Data Processor shall provide all reasonable assistance to the Data Controller in complying with its obligations under the GDPR with respect to the security of processing, the notification of personal data breaches, the conduct of data protection impact assessments, and in dealings with the ICO.

5.8 When processing the Personal Data on behalf of the Data Controller, the Data Processor shall:

5.8.1 not process the Personal Data outside the European Economic Area ("EEA") without the prior written consent of the Data Controller and, where

the Data Controller consents to such a transfer to a country that is outside of the EEA, to comply with the obligations of Data Processors under the provisions applicable to transfers of Personal Data to third countries set out in Chapter 5 of the GDPR by providing an adequate level of protection to any Personal Data that is transferred;

5.8.2 not transfer any of the Personal Data to any third party without the written consent of the Data Controller and, in the event of such consent, the Personal Data shall be transferred strictly subject to the terms of a suitable agreement, as set out in Clause 10;

5.8.3 process the Personal Data only to the extent, and in such manner, as is necessary to comply with its obligations to the Data Controller or as may be required by law (in which case, the Data Processor shall inform the Data Controller of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law);

5.8.4 implement appropriate technical and organisational measures, as described in Schedule 3, and take all steps necessary to protect the Personal Data against unauthorised or unlawful processing, accidental loss, destruction, damage, alteration, or disclosure. The Data Processor shall inform the Data Controller in advance of any changes to such measures;

5.8.5 if so requested by the Data Controller (and within the timescales required by the Data Controller) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;

5.8.6 keep detailed records of all processing activities carried out on the Personal Data in accordance with the requirements of Article 30(2) of the GDPR;

5.8.7 make available to the Data Controller any and all such information as is reasonably required and necessary to demonstrate the Data Processor's compliance with the GDPR;

5.8.8 on reasonable prior notice, submit to audits and inspections and provide the Data Controller with any information reasonably required in order to assess and verify compliance with the provisions of this Agreement and both Parties' compliance with the requirements of the GDPR. The requirement to give notice will not apply if the Data Controller believes that the Data Processor is in breach of any of its obligations under this Agreement or under the law; and

5.8.9 inform the Data Controller immediately if it is asked to do anything that infringes the GDPR or any other applicable data protection legislation.

6 Data Subject Access, Complaints, and Breaches

6.1 The Data Processor shall assist the Data Controller in complying with its obligations under the GDPR. In particular, the following shall apply to data subject access requests, complaints, and data breaches.

6.2 The Data Processor shall notify the Data Controller without undue delay if it receives:

- a subject access request from a data subject; or
- any other complaint or request relating to the processing of the Personal Data

6.3 The Data Processor shall cooperate fully with the Data Controller and assist as required in relation to any subject access request, complaint, or other request, including by:

6.3.1 providing the Data Controller with full details of the complaint or request;

6.3.2 providing the necessary information and assistance to comply with a subject access request;

6.3.3 providing the Data Controller with any Personal Data it holds in relation to a data subject (within the timescales required by the Data Controller); and

6.3.4 providing the Data Controller with any other information requested by the Data Controller.

6.4 The Data Processor shall notify the Data Controller immediately if it becomes aware of any form of Personal Data breach, including any unauthorised or unlawful processing, loss of, damage to, or destruction of any of the Personal Data.

7 Appointment of a Data Protection Officer

7.1 The Data Controller has appointed a Data Protection Officer in accordance with Article 37 of the GDPR, whose details are available from data-protection@lsbsu.org.

7.2 The Data Processor shall appoint a Data Protection Officer in accordance with Article 37 of the GDPR and shall supply the details of the Data Protection Officer to the Data Controller prior to the commencement of the processing.

8 Liability and Indemnity

8.1 The Data Controller shall be liable for, and shall indemnify (and keep indemnified) the Data Processor in respect of any and all action, proceeding, liability, cost, claim, loss, expense, or demand suffered or incurred by, awarded against, or agreed to be paid by, the Data Processor and any Sub-Processor arising directly or in connection with:

8.1.1 any non-compliance by the Data Controller with the GDPR or other applicable legislation;

8.1.2 any Personal Data processing carried out by the Data Processor or Sub-Processor in accordance with instructions given by the Data Controller that infringe the GDPR or other applicable legislation; or

8.1.3 any breach by the Data Controller of its obligations under this Agreement, except to the extent that the Data Processor or Sub-Processor is liable under sub-Clause 8.2.

8.2 The Data Processor shall be liable for, and shall indemnify (and keep indemnified) the Data Controller in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Data Controller arising directly or in connection with the Data Processor's Personal Data processing activities that are subject to this Agreement:

8.2.1 only to the extent that the same results from the Data Processor's or a Sub-Processor's breach of this Agreement; and

8.2.2 not to the extent that the same is or are contributed to by any breach of this Agreement by the Data Controller.

8.3 The Data Controller shall not be entitled to claim back from the Data Processor or Sub-Processor any sums paid in compensation by the Data Controller in respect of any damage to the extent that the Data Controller is liable to indemnify the Data Processor or Sub-Processor under sub-Clause 8.1.

8.4 Nothing in this Agreement (and in particular, this Clause 8) shall relieve either Party of, or otherwise affect, the liability of either Party to any data subject, or for any other breach of that Party's direct obligations under the GDPR. Furthermore, the Data Processor hereby acknowledges that it shall remain subject to the authority of the ICO and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a data processor under the GDPR may render it subject to the fines, penalties, and compensation requirements set out in the GDPR.

9 Intellectual Property Rights

9.1 All copyright, database rights, and other intellectual property rights subsisting in the Personal Data (including but not limited to any updates, amendments, or adaptations to the Personal Data made by either the Data Controller or the Data Processor) shall belong to the Data Controller or to any other applicable third party from whom the Data Controller has obtained the Personal Data under licence (including, but not limited to, data subjects, where applicable). The Data Processor is licensed to use such Personal Data under such rights only for the purposes of the Services, and in accordance with this Agreement.

10 Confidentiality

10.1 The Data Processor shall maintain the Personal Data in confidence, and, unless the Data Controller has given written consent for the Data Processor to do so, the Data Processor shall not disclose any Personal Data supplied to the Data Processor by, for, or on behalf of, the Data Controller to any third party. The Data Processor shall not process or make any use of any Personal Data supplied to it by the Data Controller otherwise than in connection with the provision of the Services to the Data Controller.

10.2 The Data Processor shall ensure that all personnel who are to access and/or process any of the Personal Data are contractually obliged to keep the Personal Data confidential.

10.3 The obligations set out in in this Clause 10 shall continue for a period of [insert period] after the cessation of the provision of Services by the Data Processor to the Data Controller.

10.4 Nothing in this Agreement shall prevent either Party from complying with any requirement to disclose Personal Data where such disclosure is required by law. In such cases, the Party required to disclose shall notify the other Party of the disclosure requirements prior to disclosure, unless such notification is prohibited by law.

11 Appointment of Sub-Processors

11.1 The Data Processor shall not sub-contract any of its obligations or rights under this Agreement without the prior written consent of the Data Controller (such consent not to be unreasonably withheld).

11.2 In the event that the Data Processor appoints a Sub-Processor (with the written consent of the Data Controller), the Data Processor shall:

11.2.1 enter into a Sub-Processing Agreement with the Sub-Processor which shall impose upon the Sub-Processor the same obligations as are imposed upon the Data Processor by this Agreement and which shall

permit both the Data Processor and the Data Controller to enforce those obligations; and

11.2.2 ensure that the Sub-Processor complies fully with its obligations under the Sub-Processing Agreement and the GDPR.

11.3 In the event that a Sub-Processor fails to meet its obligations under any Sub-Processing Agreement, the Data Processor shall remain fully liable to the Data Controller for failing to meet its obligations under this Agreement.

12 Deletion and/or Disposal of Personal Data

12.1 The Data Processor shall, at the written request of the Data Controller, delete (or otherwise dispose of) the Personal Data or return it to the Data Controller in the format(s) reasonably requested by the Data Controller within a reasonable time after the earlier of the following:

12.1.1 the end of the provision of the Services; or

12.1.2 the processing of that Personal Data by the Data Processor is no longer required for the performance of the Data Processor's obligations under this Agreement.

12.1.3 Following the deletion, disposal, or return of the Personal Data under sub-Clause 12.1, the Data Processor shall delete (or otherwise dispose of) all further copies of the Personal Data that it holds, unless retention of such copies is required by law, in which case the Data Processor shall inform the Data Controller of such requirement(s) in writing.

12.1.4 All Personal Data to be deleted or disposed of under this Agreement shall be deleted or disposed of in line with the SBSU Retention and Disposal of Documentation Guidelines (Appendix F).

13 Law and Jurisdiction

13.1 This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

13.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

SIGNED for and on behalf of the Data Controller by:

[insert name and title of person signing for the Data Controller]

_____

Authorised Signature

_____

Date

SIGNED for and on behalf of the Data Processor by:

[insert name and title of person signing for the Data Processor]

_____

Authorised Signature

_____

Date

SCHEDULE 1

Services

[Insert a description of the Services provided by the Data Processor (under the Service Agreement, where relevant].

SCHEDULE 2

Personal Data

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing

SCHEDULE 3

Technical and Organisational Data Protection Measures

The following are the technical and organisational data protection measures referred to in Clause 4:

1 The Data Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Data Controller, it maintains security measures to a standard appropriate to:

1.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data; and

1.2 the nature of the Personal Data.

2 In particular, the Data Processor shall:

2.1 have in place, and comply with, a security policy which:

2.1.1 defines security needs based on a risk assessment;

2.1.2 allocates responsibility for implementing the policy to specific individual or personnel;

2.1.3 is provided to the Data Controller on or before the commencement of this Agreement;

2.1.4 is disseminated to all relevant staff; and

2.1.5 provides a mechanism for feedback and review.

2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

2.3 prevent unauthorised access to the Personal Data;

2.4 protect the Personal Data using pseudonymisation, where it is practical to do so;

2.5 ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

2.6 have secure methods in place for the transfer of Personal Data whether in physical or electronic form;

2.7 password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure, and that passwords are not shared under any circumstances;

2.8 take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;

2.9 have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:

2.9.1 the ability to identify which individuals have worked with specific Personal Data;

2.9.2 having a proper procedure in place for investigating and remedying breaches of the GDPR; and

2.9.3 notifying the Data Controller as soon as any such security breach occurs.

2.9.4 have a secure procedure for backing up all electronic Personal Data and storing back-ups separately from originals;

2.9.5 have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment; and

2.9.6 adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013, as appropriate to the Services provided to the Data Controller.