EST 1892 LSBU

Data Protection Policy

Policy last reviewed	December 2021
Approved by	Group Secretary
Published on	LSBU website, Under About Us, Policies and Procedures tab. For latest version, go to: https://www.lsbu.ac.uk/about-us/policies-regulations-procedures

This Procedure is available in accessible formats on request from the Data Protection Officer. Please contact: dpa@lsbu.ac.uk

Contents

Data Protection Policy

1. Introduction

London South Bank University (LSBU) is committed to protecting personal information[1] that we may hold. This policy provides a framework to help ensure that LSBU meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

This means that personal information we are responsible for is:

- processed[2] fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

We must provide evidence to show how personal information is managed and safeguarded so that we do not put individuals at risk. There are technical and organisational measures for our systems and processes so that our employees, students, contractors, or those who process information on our behalf have access to policies, operational procedures and guidance to give them direction on the application of the information protection legislation.

LSBU usually acts as a data controller – see an explanation of the roles of controllers and processors at Annex 1.

2. Scope – Who and what is covered by this policy?

This policy covers all personal information we process about data subjects regardless of how that information is stored. This policy applies to all employees, contractors and others who process personal information on behalf of the LSBU.

The data subjects whose personal information we may process include potential employees and students, current employees and students, former employees and students, current and former workers, contractors, website users, contacts and research subjects, visitors and users of LSBU facilities.

---

[1] The UK GDPR defines personal information as information relating to an identified or identifiable natural living person – also referred to as a "Data Subject".

[2] For the purpose of the policy, processing is any activity associated with personal information and includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

3. Who is responsible for this policy?

This policy is the responsibility of the University Group Secretary but has delegated the day-to-day responsibility to the Data Protection Officer. LSBU's employees and students are responsible for the protection of personal data across LSBU. Third parties who process personal data on LSBU's behalf are also accountable for the safe processing of personal data.

4. Measures we take and tools we use to protect personal information

LSBU takes a number of measures to protect personal information. These include:

- Ensuring that employees and others with access to personal information are, given appropriate training on data protection.
- Assessing the impact of the information we intend to collect. This includes the use of Data Protection Impact Assessments (DPIA).
- Rigorous contracts with those supplying us with services to process or manage personal information on our behalf.
- Creating and maintaining records of the personal information we hold to ensure that when we have finished using this information, it is archived or destroyed securely in line with LSBU's business needs or legal requirements.
- Where an ongoing need for information is identified, but personal information is no longer required we will anonymise it[3].
- Where an ongoing need for information is identified, but personal information needs to be supressed we will pseudonymise[4] it.
- Prevention of access to personal information to people who have no legitimate reason to access it through security systems, such as CCTV, door entry and other physical and/or electronic measures.

5. Sensitive personal information

Some personal information is more sensitive and is afforded more protection. This is information relating to:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic information;
- biometric identification information[5];
- health information;
- sexual life and/or sexual orientation; and
- criminal information (convictions and offences).

[3] Anonymised data means all personal identifiable information has been removed and cannot be tracked back to the data subject.

[4] Whilst pseudonymised data is still personal, the personal identifiers are separated and replaced by, for example, a code, so that the data subject is not recognisable without the other piece of information which explains how the code works.

[5] Examples of physical or physiological biometric identification techniques include: facial recognition; fingerprint verification; iris scanning; retinal analysis; voice recognition; and ear shape recognition.

6. Your rights

The UK GDPR gives you certain rights:

1. The right to be informed – we will inform you if we are using or storing your personal information.
2. The right of access – you can ask us for a copy of your personal information by making a subject access request.
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.
4. The right to erasure – you can ask us to delete your information and, if we are able to, we will do so.
5. The right to restrict processing – you may want to stop us from using your information for some purposes.
6. The right to information 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.
7. The right to object – If you are concerned about how we are using your information tell us.
8. Rights in relation to automated decision making and profiling – if you think that we have made a decision about you automatically (by, for example a machine or computer) you can ask for the decision to be reviewed by a living person.

These rights are not absolute. Whilst you can ask for certain things to happen, there may be reasons why we cannot comply. For example, we may have to keep information that you would like deleted for legal purposes. Your rights are also included in our privacy notices but for more detailed information please refer to the Information Commissioners Office.

7. Keeping you informed

We publish information on our website and on our intranet about a number of measures we take and tools we use to protect personal information. We also publish privacy notices which explain why we collect and maintain personal information and your rights in respect of this information.

8. What to do if you want to access any of your personal information, exercise any of your rights under UK GDPR, or access third party personal information held by LSBU?

We have put forms on our website and in Annex 2 to this policy to assist you in providing the information we will need in order to locate your information. Please contact us at dpa@lsbu.ac.uk with the completed form for either a subject access request, or for any other right under UK GDPR (described in paragraph 6 of this policy), depending on your need. Please also provide proof of your identity to speed up the process.

9. What happens if you think we have not protected personal information?

If something goes wrong and you know or suspect that there has been a personal data breach[6] and personal information has not been adequately protected please let us know immediately by emailing dpa@lsbu.ac.uk

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

Examples of a data breach could be emailing the wrong person with personal data; accidentally showing a group of students each other's personal data; or even leaving personal data on a train.

We will investigate the personal information breach immediately – the sooner we can identify the location and cause of the breach, the sooner we can take corrective action to reduce the impact of the breach. Time is of the essence. Even if you think the breach is not severe, please notify us immediately.

In the first instance we will consider whether there is a risk to people, their rights and/or freedoms. We will notify individuals if they are likely to be affected. However, whilst LSBU is committed to transparency, in many instances we will not notify you if we know that the issue was contained and you will not be affected. In some instances, we may need to report the personal data breach to the Information Commissioners Office. This must be done within **72 hours** of us becoming aware of the breach.

10. Advice for Employees Who May Be Using Personal Data

There are a number of instances where employees need to consider the principles of data protection before commencing work on a project. Examples such as these could be:

- you intend to work in a project where personal data is to be processed (a research project for example);
- you are purchasing software that will process personal data; or
- you are an academic who is gathering students' details for a field trip or exam.

In instances such as these, please contact the Data Protection Officer for advice before you proceed. You will be guided to use a Data Protection Impact Assessment form (dpa@lsbu.ac.uk) or given help with a Data Sharing Agreement (govrev@lsbu.ac.uk). The Contracts team at govrev@lsbu.ac.uk can also provide contractual data protection advice.

11. Further information

A number of our related policies and procedures can be found on our website at London South Bank University, About Us, Policies and Procedures tab, Data Protection section.

[6] A Personal Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

For more details about UK GDPR, the Data Protection Act 2018 and your rights, visit the Information Commissioner's Office

For information about all UK legislation see Legislation.gov.uk

Annex 1 Controller & Processor Relationship

The UK GDPR draws a distinction between a 'controller' and a 'processor' to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility.

The UK GDPR defines these terms:

'**Controller**' means
(i) the natural or legal person, public authority, agency or other body which
(ii) alone or jointly with others
(iii) determines the purposes and means of the processing of personal data.

A controller is responsible for:
(i) complying with the UK GDPR,
(ii) able to demonstrate compliance with the data protection principles, and
(iii) take appropriate technical and organisational measures to ensure the processing is carried out in line with the UK GDPR.

Which One Am I?

To determine if you are a controller or processor, you need to consider your role and responsibilities in relation to your data processing activities. If you must decide what data to process and why – you are a controller. You are also responsible for the compliance of your processor(s) and to assess that they are competent to process personal data in line with the UK GDPR's requirements.

If you don't have any purpose of your own for processing the data and you only act on a client's instructions, you are a processor.

Controllers

Some controllers are under a statutory obligation to process personal data. Section 6(2) of the Data Protection Act 2018 says that anyone who is under such an obligation and only processes data to comply with it, will be a controller.

UK law requires auditors to be independent from their clients. This means that auditors determine why they need to use personal data and how this data is processed or stored. This independence means that auditors are considered data controllers under the GDPR.

What if two parties are in control?

If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

Joint controllers must agree between themselves who will take primary responsibility for complying with UK GDPR obligations, and in particular, the transparency obligations and individuals' rights. This information must be available to individuals. However, all joint

controllers remain responsible for compliance with the controller obligations under the UK GDPR.

Processors

A processor has more limited compliance responsibilities than a controller. Whilst still a natural or legal person, public authority, agency or other body, as a '**processor**' you process personal data on behalf of the controller and only to their instructions as the controller decides how the data is processed.

Although processors do not have the same obligations as controllers under the UK GDPR they do have a number of direct obligations. Both the ICO and individuals may take action against a processor regarding a breach of those obligations.

Annex 2: Personal Data Request Form

Data Protection contact details	**Email:**	dpa@lsbu.ac.uk
	Website:	http://www.lsbu.ac.uk/footer/data-protection

Under data protection legislation, you have the right to:

- Confirmation of whether or not LSBU processes personal data about you, and information about:
    - purposes of the processing (what we do with your personal information);
    - categories of personal data being processed e.g. name, address, academic records etc;
    - who else receives your personal data from us e.g. prospective employers, tax office/HMRC etc;
    - retention period for the personal data (how long we keep your personal information for);
    - your data protection rights (Individual rights | ICO);
    - your right to complain to the Information Commissioner's Office (ICO);
    - the source of personal data e.g. you, former education provider, employer etc;
    - whether we use automated decision-making, information about the logic involved, and the envisaged consequences for you.
- A copy of the personal data which we process about you.
- Request rectification if you think we hold incorrect information about you
- Request erasure if you do not want us to hold any information about you. However, this is subject to a number of exemptions.

LSBU has compiled this form to support you in making your request. Please complete all relevant sections, giving as much information as possible. We will use this information to help us identify the relevant personal data relating to your request.

We also need to verify your identity to make sure we only release your personal data to you, or someone who is authorised by you. If we cannot verify your identity, we will be unable to release the personal data to you.

1. Details about you (data subject)

Full name:		
Address:		
Previous address (if relevant):		
Telephone number:		
Email address:		
Reference number (e.g. staff/student number):	**Staff number**	
	Student number	

2. Your relationship with LSBU

Former, current or prospective student *(please complete section **4**)*	
employee or former employee (or contractor) *(please complete section **5**)*	
customer or other stakeholder *(please complete section **6**)*	

I am: *(please tick)*	**the data subject**	
	acting on behalf of the data subject *(please complete section **3**)*	

3. Please complete if you are acting on behalf of the data subject

Full name:	
Address:	
Telephone number:	
Relationship with the data subject: *(e.g. parent, carer, legal representative*	

You must accompany this request with evidence of your authority to act on behalf of the data subject *(e.g. evidence of permission by the data subject; a letter granting lasting or enduring power of attorney or evidence of parental responsibility).*

Please confirm that you have attached evidence of your authority toact on behalf of the data subject: *(please tick)*	

4. If you are a former, current or prospective student of LSBU:

School:	
Department:	
Course name:	
Course year(s):	
Course director:	

5. If you are or have been an employee/contractor of LSBU:

Position held:	
Department/School: ***(where applicable)***	
Line manager/School dean: **(where applicable)**	
Time period you were employed/contracted:	

6. If you are or have been a contractor or other stakeholder of LSBU:

The nature of your interaction with LSBU:	
Time period of your interaction:	

7. Details relating to the personal data:

Please confirm the right you are exercising: *(please tick)*	**Erasure**	
	Rectification	
	Access	
	Other	
Please provide further details of your request		
The personal data requested covers the following dates		
From:		**To:**

I have attached evidence of my/the data subject's identity: *(please tick) (e.g. copy of a passport/driving licence)*	

Dated:	

*****You can complete this form electronically and send it to **dpa@lsbu.ac.uk**, or manually and scan it to the same email address.