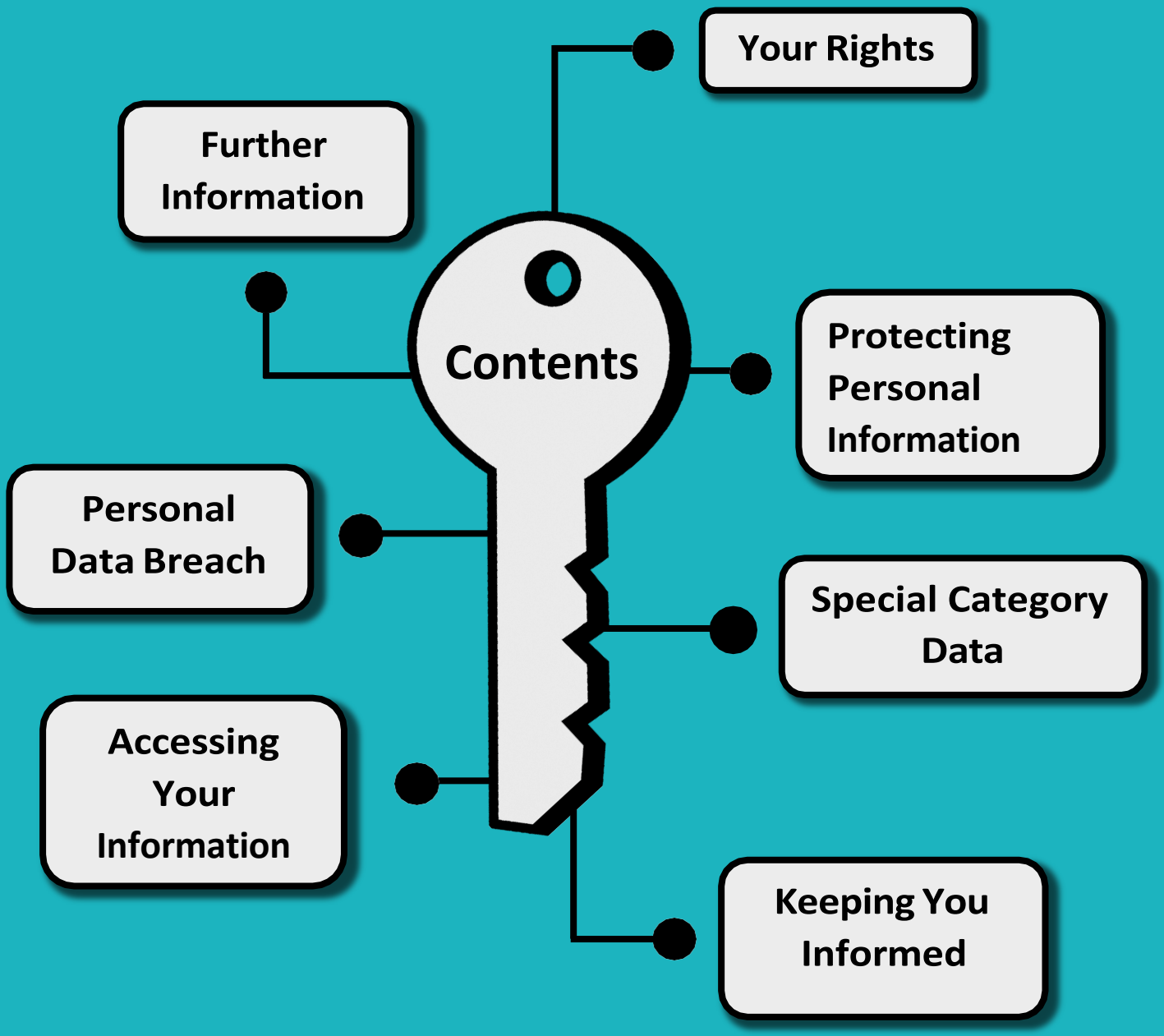
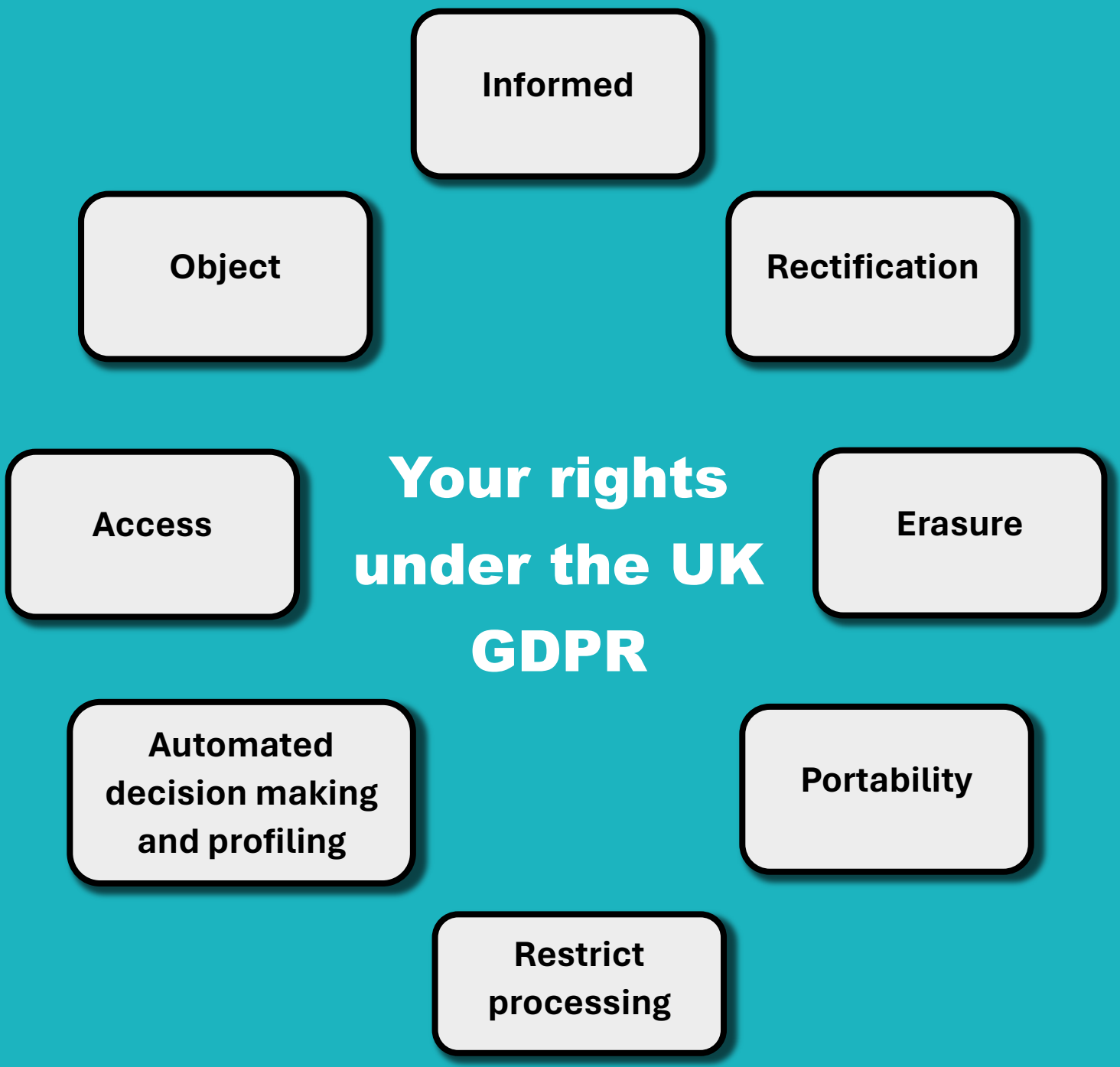
EST 1892 LSBU

Data Protection Policy

Policy last reviewed	April 2024
Approved by	Chief People and Legal Officer
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


Contents
Your Rights
Further Information
Protecting Personal Information
Personal Data Breach
Special Category Data
Accessing Your Information
Keeping You Informed

Your rights under the UK GDPR



1. Introduction

London South Bank University (LSBU) is committed to protecting all ***personal information*** related to living individuals 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 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. We put in place 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.

2. Scope

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, donors, website users, contacts and research subjects, visitors and users of LSBU facilities.

3. Who is responsible for this policy?

This policy is the responsibility of the Chief People Officer, who 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).
- Negotiating 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.
- Anonymising data where an ongoing need for information is identified, but personal information is no longer required.
- Pseudonymising data, where an ongoing need for information is identified, but personal information needs to be suppressed
- Preventing access to personal information by 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. Special Category Data

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

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic information;
- biometric identification information;
- health information;
- sex life and/or sexual orientation;

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply. For further information, please see our separate guidance Criminal Convictions Data.

6. Your rights

The UK GDPR gives you certain rights. 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 because we have another legal reason to hold it. Details of our data retention timeframes can be found in our Student and Corporate Retention Schedules. Details of your individual 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 the 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

We have provided a form on our website 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.

9. What happens if you think we haven't protected your personal information?

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 dpa@lsbu.ac.uk

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/ 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. Further information and complaints

If you want to raise a complaint about the way we have handled your personal data please refer to the Data Protection Complaints procedure

A number of our policies and procedures can be found on our website at London South Bank University . If you are unhappy about the way we are using your personal data you can raise your concerns under the Data Protection Complaints Policy.

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

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