London South Bank University

EST 1892

Data Protection Policy

2018

INTRODUCTION

London South Bank University and South Bank University Enterprises Limited ("the University", "we" or "our") obtains, uses, stores and otherwise Processes Personal Data in order to carry out its functions. The University is registered as a Data Controller with the Information Commissioner's Office.

When Processing their Personal Data, the University is obliged to fulfil individuals' reasonable expectations of privacy by complying with the General Data Protection Regulation (the GDPR), the Data Protection Act 1998 (DPA), and other relevant legislation and regulations (collectively "Data Protection Law").

The main capitalised terms used in this policy are explained in the glossary in Appendix B.

SCOPE

This policy covers all Personal Data we Process about Data Subjects regardless of the medium on which that Personal Data is stored. This policy applies to all staff, contractors and others who Process Personal Data on the University's behalf.

The Data Subjects whose Personal Data we Process include potential staff and students (applicants), current staff and students, former staff and students, current and former workers, contractors, website users, contacts and research subjects, visitors and users of University facilities.

RESPONSIBILITIES

The Executive team is responsible for driving and maintaining a culture that respects the protection of Personal Data across the University and is accountable for the University's Processing of Personal Data. The Executive lead for this policy is the University Secretary and Clerk to the Board of Governors.

All Deans and Directors of Professional Services Groups are responsible for ensuring that all University staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls and training to ensure that compliance.

Decisions taken under this policy should be risk based, with particular reference to risks to the interests and fundamental rights of the Data Subjects. Decision making should be escalated to the appropriate level based on the risks posed.

Each member of staff and others who Process Personal Data on behalf of the University (e.g. contractors, volunteers) is responsible for complying with this policy, implementing the policy in their own work, and attending the Data Protection training provided that's appropriate to their role. A failure to comply with this policy may result in disciplinary action.

The Data Protection Officer (DPO) is responsible for overseeing this policy and the processes which underpin it, developing related policies and guidelines, advising the University on its obligations under Data Protection Law and monitoring compliance. The University's DPO is Hywel Williams: dpa@lsbu.ac.uk.

POLICY STATEMENT

We will fulfil individuals' reasonable expectations of privacy by complying with the General Data Protection Regulation (the GDPR), the Data Protection Act 1998 (DPA), and other relevant legislation and regulations (collectively "Data Protection Law").

We will:

- protect individuals' Personal Data and only Process it in compliance with Data Protection Law and with good practice
- be clear about how Personal Data must be Processed and the University's expectations for all those who Process Personal Data on its behalf
- Process Personal Data effectively and efficiently to achieve the purposes for which it was obtained
- protect the University's reputation by ensuring the Personal Data entrusted to it is Processed in accordance with Data Subjects' rights
- protect the University from risks of Personal Data Breaches and other breaches of Data Protection Law and hence from liability.

The University's approach to Processing Personal Data will be guided by the Personal Data Protection Principles, which are set out in the GDPR. These require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency)
- collected only for specified, explicit and legitimate purposes and not further Processed in a manner incompatible with those purposes (Purpose Limitation)
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation)
- accurate and where necessary kept up to date (Accuracy)
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Personal Data is Processed (Storage Limitation)
- Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

The University is responsible for, and must be able to demonstrate compliance with, the data protection principles listed above (Accountability). University staff, contractors and others who Process Personal Data on the University's behalf will give effect to this policy through complying with the Data Protection Standard and related policies, procedures and processes.

DATA PROTECTION STANDARD

This standard states how we will give effect to the policy statement and comply with Data Protection Law.

1. LAWFULNESS, FAIRNESS, TRANSPARENCY

1.1. LAWFULNESS AND FAIRNESS

The University will only Process Personal Data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data for legitimate purposes without prejudicing the rights and freedoms of Data Subjects. In order to be justified, the University may only Process Personal Data if the Processing in question is based on one (or more) of the legal bases set out below. Section 4.3 below deals with justifying the Processing of Sensitive Personal Data.

The legal bases for Processing non-sensitive Personal Data are as follows:

- the Data Subject has given his or her Consent
- the Processing is necessary for the performance of a contract with the Data Subject (e.g. monitoring academic performance in order to provide the relevant qualification for which the student has enrolled) or where the Data Subject has requested the University to take specific steps before entering into a contract
- to meet our legal compliance obligations
- to protect the Data Subject's vital interests (i.e. matters of life or death)
- to perform a task in the public interest or for our official functions where the task or function has a clear basis in law
- to pursue our legitimate interests. This is only permissible in circumstances where our legitimate interests are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The specific legitimate interest or interests that the University is pursuing when Processing Personal Data will need to be set out in relevant Privacy Notices. This ground can only be relied upon for private, rather than public, functions e.g. marketing, fundraising.

We will identify the legal basis which is being relied on, and the purposes for each Processing activity, and will document them in each Privacy Notice provided to Data Subjects.

1.2. CONSENT

The University will only obtain a Data Subject's Consent where there is genuine choice and genuine control by the Data Subject whether or not to Consent to the Processing. We will rely on other legal bases where they are appropriate for the Processing.

A Data Subject Consents to Processing of their Personal Data if he/she indicates agreement

clearly either by a statement or positive action to the Processing. Silence, pre-ticked boxes or inactivity will not be sufficient. If Consent is given in a document that deals with other matters, we will ensure that the Consent is separate and distinct from those other matters.

We will enable Data Subjects to be able to withdraw Consent to Processing easily at any time and will promptly honour that withdrawal of Consent.

Where there are changes to the Processing of Personal Data which are different to and incompatible with the original purposes, we will renew the Consent prior to any Processing.

We will ensure that we gain evidence of Consent and maintain a record of all Consents obtained so that we can demonstrate compliance.

Applicable Privacy Notices will provide detail where the Data Subject's Consent is required (e.g. for electronic marketing and some research purposes).

1.3. LEGAL BASES FOR PROCESSING SENSITIVE PERSONAL DATA (SPECIAL CATEGORIES OF PERSONAL DATA UNDER THE GDPR AND CRIMINAL CONVICTIONS ETC DATA)

The University will only Process Sensitive Personal Data where it is strictly necessary to carry out a specific purpose. The Processing of Sensitive Personal Data must be based on one of the legal bases for Processing non-sensitive Personal data as well as one of the additional legal bases for Processing Sensitive Personal data.

Sensitive Personal Data is data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership

It also includes the Processing of:

- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a person's sex life or sexual orientation
- Personal Data relating to criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences

Processing Sensitive Personal Data represents a greater intrusion in individual privacy than when Processing non-sensitive Personal Data. We will therefore take special care when Processing Sensitive Personal Data, in particular in ensuring the necessity of the Processing and security of the Sensitive Personal Data.

1.4. **TRANSPARENCY (NOTIFYING DATA SUBJECTS)**

The University is required to provide detailed, specific information to Data Subjects about what happens to their Personal Data. The information provided will depend on whether the information was collected directly from Data Subjects or from elsewhere. That information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand what happens to their Personal Data. This will support the University to meet its transparency obligations.

Where Personal Data is collected indirectly (for example, from a third party or publically available source) we will provide the Data Subject with all the required information as soon as possible after collecting/receiving the data (unless notice has already been given). We will also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

2. **PURPOSE LIMITATION**

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

The University will therefore not use Personal Data for entirely new, different or incompatible purposes from those disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and where necessary has given Consent. Where the further Processing is not based on the Data Subject's Consent or on a lawful exemption from Data Protection Law requirements, we will assess whether a new purpose is compatible through following the *Change of Processing Purposes Procedure*.

Provided that prescribed safeguards are implemented, further Processing for archiving purposes in the public interest, scientific or historical research purposes, and statistical purposes will not be regarded as incompatible. We will follow the *Change of Processing Purposes Procedure* to determine whether the safeguards are adequate.

3. **DATA MINIMISATION**

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. The University will ensure that the Personal Data it Processes is adequate and relevant to the purposes for which it is intended to be Processed and will not amass large volumes of Personal Data that are not relevant for those purposes.

The University's staff and others Processing data on its behalf will only Process Personal Data when performing their job duties which require it and will not Process Personal Data for any reason unrelated to those job duties.

We will ensure that when Personal Data is no longer needed for specified purposes, it is securely destroyed or anonymised in accordance with the University's data Retention Schedules and *Personal Data Destruction Procedure*.

4. **ACCURACY**

The University will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will correct or delete inaccurate data without delay.

We will check the accuracy of any Personal Data at the point of collection and follow the procedure for reviewing the data at regular intervals thereafter.

Where a Data Subject has requested his/her Personal Data to be rectified or erased, we will follow the *Exercising Rights of Data Subjects Procedure*. Data Subjects will be notified of the outcome of their request.

5. **STORAGE LIMITATION**

The University will not keep Personal Data in a form which allows Data Subjects to be identified for longer than needed for the purposes for which the data is processed. The purposes for which the data is Processed are set out in the relevant Privacy Notices. Personal Data may need to be kept for longer in order to satisfy any legal, accounting or reporting requirements and/or risks. Were appropriate we will consider the use of Pseudonymisation and anonymization to protect Personal Data.

We will take all reasonable steps to destroy or erase from the University's systems all Personal Data that we no longer require in accordance with all relevant University records retention schedules and policies. The University has a document retention policy/schedule which can be found here [***insert link***].

We will ensure that Data Subjects are informed of the period for which their Personal Data is stored or how that period is determined by providing a link to the appropriate retention schedule in each relevant Privacy Notice.

6. **SECURITY INTEGRITY AND CONFIDENTIALITY**

6.1. **PROTECTING PERSONAL DATA**

The University will secure Personal Data by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. We will take into account the risks to Data Subjects in particular when developing, implementing and maintaining safeguards.

Safeguarding the data will include the use of encryption and Pseudonymisation where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorised to use Personal Data have access to it), integrity and availability of the Personal Data. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

University staff will be responsible for protecting the Personal Data that they Process in the course of their duties. We will therefore handle Personal Data in a way that guards against accidental loss or disclosure or other unintended or unlawful Processing and in a way that maintains its confidentiality. We will exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

University staff will comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement. These include the related policies referenced in Appendix B and all applicable processes and procedures, with particular reference to ICT policies and procedures for engaging third parties to Process Personal Data.

6.2. REPORTING A PERSONAL DATA BREACH

The GDPR requires that the University reports to the Information Commissioner's Office (ICO) any Personal Data Breach where it is likely that there will be a risk to an individual's rights and freedoms as a result of the Breach. Where the Personal Data Breach results in a high risk to a Data Subject, they also have to be notified unless certain criteria have been met. These are set out in the procedure for *Reporting a Breach of Personal Data [insert link]*.

All University staff will follow the procedures put in place to deal with any suspected Personal Data Breaches immediately following an incident and notify the DPO.

The University will retain all evidence relating to Personal Data Breaches in particular to enable us to maintain a record of such breaches, as required by the GDPR. A log of Personal Data Breaches will be maintained which will be regularly reported to the Executive.

7. TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. Personal Data is transferred when it is transmitted/sent, or viewed/accessed in a different country from where it originates.

The University will only transfer Personal data outside the EU in certain circumstances in compliance with GDPR and as outlined in our *Procedure for Engaging Third Party Contractors for Processing of Personal Data (including transfer of Personal Data overseas).*

8. DATA SUBJECTS' RIGHTS

Data Subjects have rights in relation to the way we handle their Personal Data. These are set out in Appendix C. Unless certain exemptions apply, these rights must be complied with usually within one month of receipt.

All University staff will immediately comply with the *Exercising Rights of Data Subjects Procedure* on receiving a Data Subject's request in relation to their rights.

9. DATA-SUBJECT ACCESS REQUESTS

Data Subjects have the right to receive copy of their Personal Data which is held by the University. In addition, he/she is entitled to receive further information about the University's Processing of their Personal Data as follows:

- the purposes
- the categories of Personal Data being Processed
- recipients/categories of recipient
- retention periods
- information about their rights
- the right to complain to the ICO
- details of the relevant safeguards where Personal Data is transferred outside the EEA
- any third-party source of the Personal Data

All University staff will comply with the Responding to Data Subject Access Requests Procedure.

10. ACCOUNTABILITY

10.1. APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES

The University must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The University is responsible for, and must be able to demonstrate compliance with, the data protection principles.

We will therefore apply adequate resources and controls to ensure and to document GDPR compliance including:

- appointing and resourcing a suitably qualified DPO
- implementing Privacy by Design when Processing Personal Data and completing Data Privacy Impact Assessment where Processing presents a high risk to the privacy of Data Subjects
- integrating data protection into our policies, procedures, in the way Personal Data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing, records of Personal Data Breaches
- training staff on compliance with Data-Protection Law and keeping a record accordingly
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

10.2. RECORD KEEPING

The GDPR requires the University to keep full and accurate records of all our data Processing activities.

We will keep and maintain accurate corporate records reflecting our Processing, including records of Data Subjects' Consents and procedures for obtaining Consents. We will maintain a Personal Data Processing Register which will include:

- clear descriptions of the categories of Personal Data
- categories of Data Subjects
- Processing activities
- Processing purposes
- third-party recipients of the Personal Data
- Personal Data storage locations
- Personal Data transfers
- the Personal Data's retention period and a
- description of the security measures in place.

10.3. TRAINING AND AUDIT

The University is required to ensure that all University staff and contractors undergo adequate training to enable them to comply with Data Protection Law. All staff must undergo mandatory Data Protection related training. Where appropriate training relevant to specific Processing of Personal Data will also be provided.

We will also regularly review the University's systems and processes to ensure they comply with this policy. All Staff will assist in the reviewing of systems and processes under their control.

10.4. PRIVACY BY DESIGN BY DEFAULT AND DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

The University is required to implement Privacy-by-Design measures when Processing Personal Data, by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with Data Protection principles. We will therefore ensure that by default only Personal Data which is necessary for each specific purpose is Processed, and only for the length of time necessary and with availability only to those people who have a need to access the Personal Data.

We will follow the *Data Protection Impact Assessment Procedure* [provide link] to determine which Processing of Personal Data should be subject to DPIAs. All systems Processing

Personal Data will undertake a Data Protection Threshold Assessment. The University will also conduct DPIAs in respect of high-risk Processing before that Processing is undertaken.

10.5. **DIRECT MARKETING**

The University is subject to certain rules and privacy laws, including the Privacy and Electronic Communications Regulations when marketing to our applicants, students, alumni and any other potential user of our services.

Under GDPR, the right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. A Data Subject's objection to direct marketing must be promptly honoured.

If a Data Subject opts out at any time, we will suppress their details as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

11. **SHARING PERSONAL DATA**

In the absence of Consent, a legal obligation or other legal basis of Processing, Personal Data will not generally be disclosed to third parties unrelated to the University (e.g. students' parents, members of the public, private landlords).

Some bodies have a statutory power to obtain information (e.g. regulatory bodies such as the Health & Care Professions Council, the Nursing and Midwifery Council, government agencies such as HMRC and the Child Support Agency). Further, without a warrant, the police have no automatic right of access to records of Personal Data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders.

All staff will comply with the Responding to Data Subject Access Request Procedure in disclosing Personal Data.

Some additional sharing of Personal Data for research purposes may also be permissible, subject to certain safeguards [***Refer to code of research ethics?***].

12. **CONTACTING THE DPO**

University staff should contact the DPO if they have any questions about the operation of this policy or the application of Data Protection Law or if they have any concerns that this policy is not being followed. In particular, the DPO should be contacted if:

- you are unsure of the lawful basis on which you are relying to Process Personal Data (including the legitimate interests) used by the University and any additional Processing that may be for a purpose not originally envisaged and which may not be compatible with the agreed purpose
- you need to rely on Consent and/or need to obtain Explicit Consent

- you need to draft Privacy Notices
- you are unsure about the retention period for the Personal Data being Processed (see Section below)
- you are unsure about what security or other measures you need to implement to protect Personal Data
- there has been a Personal Data Breach (through the process set out in the Reporting a a Breach of Personal Data procedure)
- you are unsure on what basis to transfer Personal Data outside the EU
- you need any help dealing with any rights invoked by a Data Subject
- whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes other than for which it was collected
- you plan to undertake any activities involving Automated Processing including Profiling or Automated Decision-Making
- if you need help complying with applicable law when carrying out direct marketing activities
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (such as overseas partners, agents, and organisations conducting surveys on the University's behalf).

13. CHANGES TO THIS POLICY

The University reserve the right to change this policy at any time without notice to you so please check regularly to obtain the latest copy.

We last revised this policy on [***date***] [and made the following changes: [***details of changes].*** The policy will be reviewed annually.

APPENDIX A

SUPPORTING DOCUMENTS FOR THIS POLICY

[internal procedures]

RELATED POLICIES

Freedom of Information Policy
ICT- Acceptable Use Policy
ICT-Account Management Policy
ICT- Email Usage Regulations policy
ICT – IT Information Security Policy
Mobile Device Policy
Policy and Standards for CCTV Operation at LSBU
Records Management Policy
Research – Data Management Policy
Safeguarding Policy

DOCUMENTS SUPPORTING RELATED POLICIES

Corporate Records Retention Schedule (being revised)
Student Records Retention Schedule (being revised)

APPENDIX B

Glossary of Terms

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including Profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Profiling: any form of Automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to Process Personal Data. It is responsible for establishing practices and policies in accordance with the GDPR. The University is the Data Controller of all Personal Data relating to its Processes and used delivering education and training, conducting research and all other purposes connected with it including business purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

Data Privacy Impact Assessment (DPIA): tools, assessments, and processes used to identify and reduce risks of a data Processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Law: includes the General Data Protection Regulation, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations.

Data Protection Officer (DPO): the person appointed as such under the GDPR and in accordance with its requirements. A DPO is responsible for advising the University (including its employees) on their obligations under Data Protection Law, for monitoring compliance with Data Protection Law, as well as with the University's polices, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, Personal Data, where that breach results in a risk to the Data Subject. It can be an act or omission.

Privacy by Design and Default: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR prior to Processing.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the University collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee, student and donor Privacy Notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to Personal Data from its creation to its destruction, including both creation and destruction.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or Pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

APPENDIX C: Data Subjects' Rights under GDPR

The right to be informed	Individuals have a right to clear and concise information about what we do with their personal data. Individuals should be told before we use their data.
The right of access	Individuals have a right to access their personal data and to be assured that the processing of their data is fair and lawful.
The right to rectification	Individuals have a right to have their personal data corrected if it's inaccurate, or completed if it is incomplete.
The right to erasure	Individuals have a right to have their personal data erased in certain circumstances – 'the right to be forgotten'.
The right to restrict processing	Individuals have the right to request the restriction or suppression of their personal data in certain circumstances. (Hold the data but not use it, usually for a period of time pending other decisions)
The right to data portability	Individuals have a right to obtain and reuse their personal data across different services. (Move, copy or transfer personal data easily from one IT environment to another safely and securely without affecting the usability of the data)
The right to object	Individuals have a right to object to processing of their personal data where the processing is based on legitimate interests or performance of a public interest task, or where the processing is for direct marketing or scientific/historical research and statistics.
Rights related to automated decision making and profiling	Individuals have a right not to not have decisions with legal or similar effects made about them solely using automated processing (including profiling), unless certain exceptions apply.