Data Protection Policy			
Document type:	Policy		
Document number:	IT-162	Version:	03
Department:	Information and Technology		
Approved by:	Executive Board	Date approved:	10/11/2025
Effective from:	10/11/2025	Review date:	10/11/2028
Publication:	SOAS website		
Related documents:			
Documents replaced:	IT-158-02 Data Protection Policy		
Note: All policies must be read in conjunction with all other SOAS policy, procedure and guidance documents. Printed copies of policies may not be the most up to date, therefore please refer to the policy pages on the SOAS external website or intranet for the latest version.			

1. Introduction

1.1. In order to carry out the University's business, SOAS University of London ("SOAS") needs to collect and work with certain types of Personal Data about the people with whom it deals, such as current, past and prospective students, employees, and those with whom it communicates. This information is collected for administrative purposes (such as staff recruitment and the administration of programmes of study) and to fulfil legal obligations to regulatory bodies and the government.

1.2. Data Protection Legislation requires that this Personal Data must be processed lawfully, stored safely and not disclosed to any other person or body unless it is necessary to fulfil a contract, meet a legal obligation, or you have asked us to. SOAS is committed to protecting the rights and privacy of individuals in accordance with the requirements of the law. This document outlines SOAS's policy in relation to the current law.

2. Scope

2.1. The Personal Data Processing carried out by SOAS is governed by the provisions of the Data Protection Legislation.

2.2. SOAS is the Data Controller in respect of Personal Data which is Processed in the course of the University's business. SOAS's business comprises:

- teaching
- pedagogic and learning support
- research
- enterprise and knowledge exchange
- human resource administration (including recruitment)
- student recruitment and admissions
- services supporting the student and academic experience

- student registration, progression, and assessment
- external engagement and advancement
- alumni community management
- financial management
- estates and facilities management
- IT support
- legal compliance and corporate governance, and
- marketing and communications

2.3. SOAS is registered as a Data Controller with the Information Commissioner's Office. The ICO registration number is Z6740574.

2.4. SOAS's Data Protection Officer is the Information Compliance Manager, whose role is to inform and advise the University about, and to ensure that the University remains compliant with, Data Protection Legislation.

2.5. If you Process Personal Data in the course of SOAS business, the Processing falls within the scope of this Policy. You have a responsibility to keep Personal Data safe and to only Process Personal Data in accordance with this Policy and the Data Protection Legislation.

2.6. Any action by an individual which is in breach of this Policy may result in SOAS being found liable in law for a breach of the Data Protection Legislation. SOAS may be subject to an administrative fine issued by the UK regulator, the Information Commissioner's Office, or, where an individual or group of individuals prove they have suffered material or non-material damage as a result of an infringement of the Data Protection Legislation caused by SOAS, they may seek to claim compensation from the University.

2.7. Accordingly, any breach of this Policy will be considered a disciplinary offence and the infringing individual may be subject to the provisions of the relevant staff or student disciplinary procedure.

2.8. SOAS is not responsible for any Processing of Personal Data carried out by staff which is not related to their employment with SOAS, even if the Processing is carried out using SOAS equipment and facilities. Staff are personally responsible for complying with the Data Protection Legislation with regards to Personal Data for which they are the Data Controller.

2.9. SOAS is not responsible for Personal Data Processed by staff which has been permitted by SOAS and is carried out on SOAS systems but is for the purpose of fulfilling a role on behalf of another organisation (e.g. Processing carried out by trade union branch representatives solely in their capacity as a representative, or processing by the SOAS Student Union). The Data Controller shall be the organisation on whose behalf the data is being Processed.

2.10. Any questions or concerns you have about the content of this Policy or SOAS' Processing of your Personal Data can be directed to the Data Protection Officer by email at dataprotection@soas.ac.uk, by telephone at 020 7898 4817, or by post to:

Information Compliance

SOAS University of London

10 Thornhaugh Street

Russell Square

London

WC1H 0XG

3. Definitions

- **Criminal Offence Data**: Personal Data relating to the alleged commission of offences by the Data Subject, or proceedings for an offence committed or alleged to have been committed by the Data Subject or the disposal of such proceedings, including sentencing.
- **Data Breach**: 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.
- **Data Protection Legislation:** the General Data Protection Regulation (EU 2016/679) (GDPR) and the Data Protection Act (2018) (DPA), as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 2018
- **Data Subject**: the identified or identifiable living individual to whom Personal Data relates
- **High Risk Processing**: is any operation where the categories of Personal Data or nature of the operation will result in a high risk to the rights and freedoms of Data Subjects. Such operations may include but are not limited to: large scale Processing of Special Category Data; monitoring Data Subjects on a large scale; systematic or extensive profiling or automated decision-making to make significant decisions about individuals, particularly where those decisions have legal implications for the individual; using new technologies to Process Personal Data; combining, comparing and matching Personal Data from multiple sources; routine online or offline tracking of a Data Subject's location and behaviour.
- **Personal Data**: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- **Processing**: any operation on Personal Data, including obtaining, recording, holding, organising, structuring, storing, adapting or altering, retrieving, consulting, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, and destroying the data.
- **Special Category Data**: Personal Data relating to racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health (including disabilities), sexual life, sexual orientation, biometric and genetic data where it could lead to the identification of the Data Subject.

4. Roles and responsibilities

4.1. SOAS is responsible for discharging its responsibilities and understanding its liabilities as a Data Controller under the Data Protection Legislation

4.2. SOAS is responsible for ensuring that we put in place appropriate technical and organisational measures to protect Personal Data

4.3. The measures SOAS will take to protect Personal Data take into account the nature, scope, severity and context of Processing as well as the risks of varying likelihood and severity to the rights and freedoms of Data Subjects

4.4. SOAS's Chief Information Officer is responsible for SOAS's cyber security resource to ensure our networks are secure and to provide a level of defence proportionate to the risk posed by the nature of our Processing and the Personal Data Processed. SOAS's Director of Human Resources is responsible for embedding mandatory data protection training for all new staff, and for ensuring all staff, contractors and agents employed by the University are subject to a duty of confidentiality in relation to Personal Data they work with.

4.5. SOAS is responsible for designing systems, processes and services which make data protection an essential component of their core functionality. The University proactively anticipates data protection risks and privacy-intrusive events by integrating our Data Protection Impact Assessment into technology work requests, procurement due diligence processes, and our Research Ethics procedures. The Chief Information Officer and Director of Finance and Procurement are jointly responsible for ensuring specifications for data security, availability and integrity are built into the University's procurement due diligence processes. The Director of Research and Enterprise is response for the Research Ethics procedures

4.6. SOAS respects the data protection principles of data minimisation and purpose limitation in all of our Processing activities, by ensuring data collection tools capture no more data than the minimum required for the purpose, and that personal data collected for a specific purpose is not Processed for a further incompatible purpose. In some circumstances, additional privacy controls such as pseudonymisation may be implemented to minimise the Personal Data Processed.

4.7. We have a responsibility to choose our Data Processors carefully. When procuring a new system or service which will involve a third-party Processing Personal Data on our behalf, we will take steps to ensure the Data Processor provides sufficient guarantees of their technical and organisation measures for data protection by design. The Director of Finance and Procurement is responsible for ensuring data Processing terms consistent with Article 28 of the GDPR are written into SOAS's commercial terms and conditions.

4.8. The Data Protection Officer is responsible for ensuring SOAS maintains a complete record of our Processing activities, and other records pursuant to Article 30 of the GDPR on Documentation as required.

4.9. SOAS follows a procedure for reporting Data Breaches which is consistent with the provisions of Articles 33 and 34 of the GDPR. The Data Protection Officer is responsible for promoting

and monitoring the effectiveness of the Data Breach Reporting Procedure which is available on the SOAS website here https://www.soas.ac.uk/infocomp/dpa/databreaches/

4.10. SOAS has established an internal procedure for handling complaints related to data protection to reassure members of our community and the public that any complaint about the lawfulness of the University's Processing will be handled in a consistent, fair and equitable manner. The Procedure is published on our website here: Data Protection Complaints Procedure | SOAS

4.11. As a public authority, SOAS has fulfilled its legal obligation to appoint a Data Protection Officer (DPO). The DPO's role consists of at least the following tasks:

- to inform and advise SOAS and its employees who carry out Processing of their obligations under data protection legislation;
- to monitor compliance with the GDPR, with the policies of SOAS in relation to the protection of Personal Data, including the assignment of responsibilities, awareness-raising and training of staff involved in Processing operations, and information audits;
- to provide advice where requested with regards to the Data Protection Impact Assessment and monitor its performance under Article 35 of GDPR;
- to cooperate with the Information Commissioner's Office (ICO);
- to act as the contact point for the ICO on issues relating to Processing, including the prior consultation referred to in Article 36 of GDPR relating to High Risk Processing, and to consult, where appropriate, on any other matter.

4.12. The DPO at SOAS is given the required independence to perform their tasks, and is not subject to any conflict of interest in the performance of their role (such as determining the means and purposes of Processing, by having authority to choose system providers or chairing project boards).

4.13. The DPO must report to the highest level of management. SOAS's DPO reports to Executive Board on data protection activities and risks on an annual basis.

4.14. New and revised procedures concerning data protection, and measures taken to operationalise such procedures, are within the remit of the IT Governance Group, which meets on a monthly basis.

4.15. Directors of Professional Services (DOPS) and Academic Heads of Department (HODs) are responsible for ensuring their staff manage records in accordance with SOAS's Records Management Policy and Corporate Retention Schedule. DOPs and HODs should, with the support of the DPO, implement procedures and processes which support compliance with the Records Management Policy and Corporate Retention Schedule

5. What Personal Data do we process, and how and why do we process it?

5.1. SOAS Processes many types of Personal Data, for a variety of different purposes. When SOAS Processes Personal Data we will only do so when it is absolutely necessary to fulfil our contractual obligations, to carry out our public tasks as a public authority, or to achieve a beneficial purpose for the University and the members of our community.

5.2. Information about the types of Personal Data we Process, the contexts in which we Process Personal Data, the purposes of our Processing and lawful basis for Processing, information on Data Subjects' rights and any sharing of Personal Data with third parties, and how long we retain data, can be found in our Privacy Notices which can all be accessed on the SOAS website here: https://www.soas.ac.uk/infocomp/dpa/privacy-notices/. The Privacy Notices currently published by SOAS are:

- Staff Privacy Notice
- Job Applicants' Privacy Notice
- Student Privacy Notice
- Alumni, Donors and Supporters Privacy Notice
- Enquirers, Applicants and Offer-holders Privacy Notice
- Events and Conferences Privacy Notice
- Widening Participation Privacy Notice
- Trustees Privacy Notice
- Web Privacy Policy
- Postgraduate surveys notice

5.3. SOAS will, where necessary, Process Special Category Data or Criminal Offence Data for various purposes, including but not limited to Processing necessary to comply with employment law or social protection law; health purposes, including provision of occupational or preventative medicine and assessing the working capacity of an employee; archiving in the public interest or research and statistical purposes; or other purposes carried out in the substantial public interest, such as monitoring the equality of opportunity and treatment at the University, and putting in place measures to uphold such equality of opportunity and treatment.

5.4. Where SOAS Processes Special Category Data or Criminal Offence Data we inform Data Subjects in our published Privacy Notices

5.5. SOAS is required under Schedule 1 Part 4 of the DPA to have in place an Appropriate Policy document for Special Category Data or Criminal Offence Data Processed for the purposes of complying with employment law or social protection law, or where Processing is carried out for a Substantial Public Interest condition (except where the Processing involves making a disclosure to a law enforcement agency for the purpose of preventing or detecting unlawful acts).

6. Who do we share data with?

6.1. To support our essential services and comply with regulatory or statutory requirements, SOAS needs to share Personal Data with third parties.

6.2. When we share Personal Data with third parties routinely, we will enter into an agreement which sets out the roles and responsibilities of each party, the technical and organisational measures in place to safeguard personal data, the details of the data sharing under the Agreement, and sets out the legal rights and judicial remedies available to Data Subjects under the Data Protection Legislation.

6.3. When we share Personal Data with third parties occasionally, we will do so in accordance with our Information Sharing Protocol

6.4. We will maintain records of all incidences of data sharing with third parties, recording what was shared, with whom, the timing and duration of the sharing, the purpose and necessity of sharing, and any plans for the destruction or return of the Personal Data once the purpose of the Processing is fulfilled.

7. International transfers

7.1. Where it is necessary for SOAS to make a restricted transfer of Personal Data to a territory outside of the United Kingdom (a 'Third Country'), we will do so in accordance with the following conditions:

- The Third Country has received an adequacy regulation from the UK Government, meaning their national laws give Data Subjects a level of data protection rights and freedoms equivalent to UK law.
- The transfer is carried out in accordance with one of the safeguards provided in Article 46 of the UK GDPR
- The transfer is occasional, and can be carried out in accordance with one of the exceptions in Article 49 of the UK GDPR

7.2. SOAS will not rely on the exceptions allowing transfers on condition of the explicit consent of the data subject or to fulfil a contractual obligation where the University is pursuing one of its public tasks, in accordance with Article 49(3) of the UK GDPR.

8. How long do we retain personal data?

8.1. SOAS must comply with the data protection principle of storage limitation in order to protect Data Subjects from risks associated with the retention of outdated and erroneous Personal Data. Retention of Personal Data beyond the period established in SOAS's Corporate Retention Schedule could lead to detrimental consequences to the Data Subject if a decision is made based on incorrect data, or the University uses inaccurate contact details to get in touch with the Data Subject. Retaining greater volumes of Personal Data than is necessary to achieve our purposes also increases the risk to the Data Subject in the event of a Data Breach.

8.2. All staff should review their records at set intervals in the year, and identify the retention policy for each category of record for which they are responsible. Records which have reached their disposal date should be reviewed where necessary, and then securely destroyed. Periodic reviews should be carried out according to the records owned by the specific Directorate, but may take place at: the end of the tax year; end of the financial year; end of the academic year; and the end of the calendar year. Directors of Professional Services are responsible for ensuring their records are managed in accordance with the retention policies.

8.3. SOAS's retention policies for each category of record created by the University are set out in our Corporate Retention Schedule.

9. Your data protection rights

9.1. Under the data protection legislation Data Subjects have certain rights in relation to their Personal Data. The rights allow Data Subjects to ask SOAS to take specific actions in relation to the Personal Data Processed by the University. SOAS will ensure that we comply with these requests within one month of being asked, although if the request is very complex we may ask for a little more time (up to a maximum of two further months). These rights are:

9.2. **The right to be informed**: If you have supplied us with Personal Data directly, you have the right to be told who we are, why we are Processing your data, our reason for doing so, whether we share the information with third parties, and if so who those third parties are, how long we hold onto the data for, and whether we transfer any of your data outside of the European Economic Area. We will tell you all this at the time we collect your data

9.3. If your Personal Data has been given to us by a third party, we will tell you who those sources are, and we will tell you the categories of Personal Data we are Processing. This information will be given to you within one month of us receiving it, unless you already have the information, it is exempt under a condition in Schedules 2-4 of the DPA, it would be detrimental to the objective of the Processing, or we are subject to an obligation of professional secrecy governed by law.

9.4. Our Privacy Notices provide all this information to Data Subjects. There is a different Privacy Notice for each group of individuals in our community, or where data is Processed in accordance with our public facing activities (for instance running events and conferences, or running our website).

9.5. The relevant notice is provided directly to Data Subjects at the point data is collected, and all notices are reasonably accessible through our website. Data Subjects will be informed by the most appropriate medium (such as a news item in existing newsletters) of any major changes to our Privacy Notices, such as changes to reflect a new purpose of Processing.

9.10. **The right to access data we hold about you ("right of access"):** You have the right to request a copy of the information we hold about you to check that we are Processing your data lawfully. Guidelines on how to exercise this right at SOAS, and for information on the exceptions to this right, are published on our webpage: Requesting access to Personal Data.

9.11. **The right to correct data we hold about you ("right to rectification"):** If you find that any of the data we hold about you is factually incorrect, you can change it yourself (if you have access to a self-service system) or ask us to change it for you.

9.12. **The right to ask us to restrict the processing of your data ("right to restrict processing"):** If you have challenged the lawfulness of our Processing or feel that we hold inaccurate Personal Data which could affect your rights, you can ask us to restrict Processing (we will hold it to enable us to flag the data as restricted, but will not use it) while we resolve the issue.

9.13. **The right to request erasure of your data, or withdraw consent from direct marketing ("right to erasure"):** If you withdraw your consent and want us to forget you, or we have finished Processing your data under contract or for our operational needs and no longer need it, you can ask us to erase it.

9.14. **The right to request a copy of the data you provide us with in machine readable format, or to request that we transfer a copy of the data to another IT environment ("right to portability"):** If you have supplied us with automated data by consent or under contract, you can request a copy of the data in an open-source machine readable format which would allow it to be transferred directly into another IT environment, or you can ask us to transfer it directly.

9.15. **The right to object to processing of your data, or withdraw consent from direct marketing ("right to object"):** You can object to our Processing of your personal data for any reason relating to your situation. If we are Processing your data because it is in our legitimate interests or we are doing so in our official authority as a public body, we will consider whether your rights and interests override the University's interests.

9.16. **The right to be informed of any automated processing or profiling which takes place at SOAS ("rights related to automated decision-making including profiling"):** Automated processing or profiling may be carried out by the University to make significant decisions about you, but only if we put in place safeguards, which:

(a) provide you with information about those decisions and what they mean,

(b) allow you to make representations on those decisions,

(c) ask for a human to intervene and review the decision, or

(d) allow you to contest the decision.

9.17. We will not use Special Category Data to make significant decisions about you based on automated decision-making or profiling unless:

(a) We have your explicit consent

(b) It is necessary for the performance of a contract between you and SOAS

(c) It is required or authorised by law

9.18. The right to be informed, to request access to your data, to correct your data, and to be informed of automated Processing which might affect you are absolute rights, and are always available to Data Subjects.

9.19. The rights of restriction, erasure, portability and objection are not always available, and depend on SOAS's lawful basis for Processing your data. The specific lawful basis we give to justify our Processing of your Personal Data will be stated in the Privacy Notice which applies to your situation.

9.20. The appropriate point of contact to exercise each of these rights is provided in the Privacy Notice which applies to the Data Subject.

10. Who is responsible for regulating data protection?

10.1. The body which regulates data protection in the UK is the Information Commissioner's Office (ICO). The ICO can be contacted separately for advice about how the data protection legislation protects individuals' Personal Data. If you are a Data Subject and believe SOAS is processing your data unlawfully, you can make a complaint to the ICO by visiting their website: https://ico.org.uk/, or by calling 0303 123 1113