



UNIVERSITY OF LONDON

Staff Privacy Notice

1. Introduction

This privacy notice provides information about the use of personal data while you are a current or former member of staff of the University of London. This includes while you are a full-time, part-time permanent or fixed-term employee, in clerical, technical, administrative, professional and academic roles, freelancers, independent contractors, affiliated lecturers or academic visitors, academic contractors, consultants or other outsourced and non-permanent workers.

The data controller processing your data is the University of London. We are registered as a data controller with the Information Commissioner's Office (our registration number is Z5419651) and we are committed to ensuring that the personal data we process is handled in accordance with data protection legislation. You can contact our Data Protection Officer at data.protection@london.ac.uk or via the postal address of:

FAO Data Protection Officer

University of London
Senate House
Malet Street
London WC1E 7HU.

Further information is available on the [Policies website](#).

You might find you are given additional privacy notices as you engage with different areas or use different services at the University of London.

2. What information do we collect from you?

While you work for, or with, the University of London we will collect, obtain and hold a range of data about you that may be able to identify you directly or indirectly. This data is personal data. When you cease to be employed or engaged by us, we will continue to hold some data about you in accordance with our retention schedules to fulfil our remaining tasks and obligations.

The personal data that the University holds about you as a member of staff includes the following:

Personal information

Your name

Photograph

Employee username

ID number

Date of birth

Gender

Nationality

National insurance (NI) number

Copies of documentation proving your right to work such as your passport or visa

Contact details (included a personal telephone number if you have given it to us)

Dietary requirements

Details of your right to work in the UK and your immigration status (where applicable)

Passport details

Job information

Your role title and department

Information about your employment contract such as:

- Start date/s
- Hours
- Contract type
- Salary

Information about any benefits you have received

Details of periods of leave taken by you, including:

- Holiday
- Sickness absence
- Family leave
- Sabbaticals
- Your bank details

Performance information

Assessments of your performance, including:

- Appraisals
- Performance reviews and ratings

- Training you have participated in
- Performance improvement plans
- Promotions
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.

Education and work history

Details of your:

- Qualifications
- Skills
- Experience
- Employment history
- References given and received
- Research proposed or undertaken.

Information about your family, lifestyle or social circumstances

In certain circumstances we will also hold limited information about your spouse, partner, or civil partner, or other individuals. This is collected, for example, where you name them as an emergency contact or where shared parental leave is requested.

Information about your activities in the University

This includes

- use of information and communication systems, such as CCTV footage and access times from swipe card access,
- IP address if you access information from a device,
- Participation in recorded teaching activities, including webinars, where your voice and/or image are recorded.

Special category data

The University may also process some kinds of more sensitive information about you, called “special category” data in Data Protection legislation. Special Category data receives extra protection under data protection law. The Special Category data we may process about you includes data about:

- Health, medical conditions or disabilities
- Religion or beliefs
- Ethnicity

- Political opinions
- Sexual orientation
- Trade union affiliations, where applicable.

For certain roles, we seek information about past criminal convictions, working with children or vulnerable adults, and/or your fitness to practise in certain regulated professions.

3. How do we collect information about you?

We ask you to provide much of this data to us directly when you start your employment. We also collect data from you during your employment with us in relation to your activities as a member of staff. You might provide it to us independently for us to help you with something. We also generate some data about you ourselves (such as your employee ID and username).

We collect data from you when you:

- Submit an application for a job at the University
- Complete your new starter and payroll forms and starting working with us
- Update your personal record via the Human Resources Employee Self Service system during your employment or ask us to update your record in any way
- Supply emergency contact details - in which case we will assume that the person whose details you give us are happy for these details to be shared with us by you
- Request shared parental leave, in which case we will receive the spouse/partner's name and the name of their employer either from you or from your spouse/partner's employer
- Share it during the course of your employment, for example, during correspondence with you, during the annual appraisal process, if you need to take sick leave, or if your role changes

The University works closely with third parties (including employment agencies, partner organisations, pensions scheme providers, and compliance services such as UKVI, Disclosure and Barring Service, and agencies that provide services such as Right to Work Checks). We may receive information about you from them, including special category personal data or criminal convictions data.

In particular we may receive the following information from third parties:

- CVs
- Details of your right to work in the UK
- Immigration status

- DBS certificate number
- Other information in connection with your activities as a member of staff at the University of London.

4. Why do we collect this information?

Overall, we use your personal data to manage your relationship with us as a member of staff at the University of London. Data Protection laws require us to meet certain conditions before we are allowed to use your personal data. This includes having a 'legal basis' for the processing, depending on the reason why we use the data. Below we will explain the main purposes for which we use your data, and the legal basis under which we process it.

Necessary for the University to comply with a legal obligation

We process data about you under this legal basis when we need to do so to comply with our legal obligations, such as in the areas of employment for tax purposes or to comply with the Equality Act, or laws around health and safety in the workplace.

Necessary for the University to perform a contract with you

We process your data in order to carry out the contract of employment we have with you, or to enter into it in the first place – for example, ensure you can work in the UK, pay you a salary and keep records of university procedures that may concern you such as grievance proceedings, disciplinarys and changes to your employment such as promotion, pay rises, location changes. These examples are not exhaustive.

To meet our public task

We process your data to ensure that we can carry out our role as an educational and research establishment, meeting legal, moral and contractual obligations as laid out in the University's Statutes and Ordinances.

We process data to meet this public task role when we carry out activities to meet our teaching, learning, research and innovation obligations such as:

- Teaching on undergraduate, postgraduate and short courses, including making recordings of webinars and other similar teaching activities
- Carrying out activities to facilitate the provision of educational courses, such as teacher development
- Facilitating and carrying out research, including research in partnership with other organisations, and research funded by private organisations
- Quality assurance processes around development and upkeep of courses and modules.

Processing in the legitimate interests of the University or other people

Sometimes we will process your data because we have identified a 'legitimate interest' in doing so. The legitimate interests we identify are determined through an assessment made by weighing our requirements against the impact of the processing on you. This is done to make sure that our legitimate interests will never override your right to privacy and the freedoms that require the protection of your personal data.

Examples of when we will process your data in our legitimate interests are:

- Providing you with a university campus card, University of London IT account, access to a University of London email account, and give you personalised access to buildings, IT applications, resources and network services such as WiFi
- Monitoring use of IT services to ensure adherence to the University's Acceptable Use Policy
- Providing you with access to training and development services
- Enabling effective communications to you about security or operations and to keep you informed and involved with what's happening at the University. This may continue after you have left the University if we feel the occasion is applicable to leavers.
- Contacting those people you have named to be notified in the event of an emergency.
- Operating and keep a record of employee performance and related processes to plan for career development, succession planning and workforce management purposes.
- Providing a reference to third parties such as future employers
- Using staff information to conduct strategic analysis, modelling and forecasting to help the University plan ahead.
- Analysing the effectiveness of a service that we provide. This analysis is carried out at an aggregate level so that you are not identifiable from the data.
- With the University's insurance brokers and insurers and related third parties, e.g. lawyers and loss adjustors for the purpose of risk mitigation, securing insurance cover, maintaining and administering that cover and processing any claims that may arise as a result.

Necessary to protect your vital interests or those of another person

On rare occasions, we may need to access or share your information to protect your life or that of another person, for example in an emergency where we cannot gain your consent or to do so could endanger life. We will only rely on vital interests in extremely limited circumstances when no other legal basis is available.

You have given us your consent to process your data for a specific purpose

We may sometimes ask for your consent to do something that involves use of your personal data. In some cases we might process your special category data with your consent. We will do this where no other lawful basis applies and where it makes sense to give you the highest level of control over how your data is used by us.

For this reason, we will not ask for your consent very often where your data is being processed for employment reasons because one of the other lawful bases listed above will often be more appropriate. However, you would be asked to specifically consent to the processing of your data in certain circumstances. These include if we wish to send you marketing, to use your voice or image in publicity material, or to process your data where we cannot rely on one of the above bases. If we do process your personal and special category data based on your consent you will have the right to withdraw your consent at any time (see the section below on your rights under data protection law).

3.1 Processing your ‘special category’ personal data

Sensitive personal data, called “special category” data in the legislation, receives extra protection under data protection law. The University can only process it if we have an additional lawful basis to rely on and meet higher standards for safeguarding it.

We process your Special Category data when we use it in relation to the following legal bases

To meet employment obligations, and obligations under social security and protection law

This applies when we:

- Keep a record of reasonable adjustments for a disability to allow us to meet our obligations under equalities legislation
- Monitor our compliance with our responsibilities under equalities legislation
- Set up a voluntary salary deductions to a trade union
- Carry out a DBS check as part of the assessment of suitability during your application to work at the University of London
- Record details of absences from work (other than holidays) including time on sick leave or statutory / family leave.
- Record your reason for leaving employment where the reason is determined to be related to your physical or mental health or wellbeing.
- Process data about you to meet other obligations under employment law.

For purposes of preventive or occupational medicine and to assess your working capacity as an employee

This applies when we

- Support your training, health, safety and welfare requirements, including by making appropriate referrals to the Occupational Health service
- obtain advice from medical professionals, such as occupational health or GPs, with regards to making adjustments to your working practices due to ill health.

Provide counselling

We may process data relating to physical or mental health or wellbeing to provide you with counselling services

To establish, exercise or defend legal claims against the University.

We rely on this basis when we process your personal data in relation to a legal claim.

To protect your life or someone else's

We rely on this basis on rare occasions when we cannot reasonably get your consent in a situation where you are putting your own or another person's life at risk.

For statistical purposes

We use this when we collate and analyse your data to improve our internal processes or to meet external initiatives such as Athena Swan or the Race Equality Charter. We always ensure that your right to data protection is respected, and we ensure that only the minimum of data needed is used for these purposes

In the substantial public interest

We process your data in the substantial public interest when we

- Secure, maintain and administer insurance cover for the general protection of the University and its staff.
- Process insurance claims and enable staff to access the University of London's insurance whilst on approved business or field trips abroad.

4. How long do we keep your information?

As a principle, information about you will not be kept for longer than it is needed for the purpose it was collected. You can find specific information about the lengths of time for which the University keeps your data detailed within the Retention Schedules available on the staff intranet page. When it is no longer required in line with its retention period, personal information is securely and permanently destroyed. Some basic information about our former staff is transferred to the University Archives for permanent preservation in the long term historical interest.

5. Who do we share your information with?

While you are working with us, we will need to share certain information both internally between departments and with external parties. As a principle, only minimal information will be shared as necessary and only where we have identified a lawful basis or exemption for doing so. The data we share internally will always be proportionate to the need.

Some information must be shared by HR with other departments to complete essential tasks related to your employment, such as payroll, legal, finance, occupational health, pensions and arranging access to IT services.

Other purposes for which personal data may need to be shared between internal departments include:

- Analysis to ensure our compliance with equality of opportunity and diversity legislation
- Allow for line managers to provide staff with sufficient support in their role
- Strategic analysis, planning and forecasting
- Investigating alleged employee misconduct

Sharing data about staff with third parties

Your personal data may be disclosed to other organisations as required by law, for crime prevention and detection purposes, and to protect your vital interests. We share with the following third parties for these purposes:

- HMRC, the Higher Education Statistics Agency (HESA) or Health and Safety Executive (HSE) to meet statutory reporting obligations
- External pensions providers to administer staff pensions
- Disclosure and Barring Service to obtain criminal record checks for certain roles
- Law enforcement agencies for the prevention or detection of crime
- External auditors
- Legal advisors to the University, and courts of law as necessary

- Emergency response services as necessary to protect your vital interests or those of another person
- Public Health England/NHS track and trace or any appropriately designated body, when we are requested to do so

Where necessary, we may also share your information with:

- Third parties who carry out aspects of processing on our behalf, such as mailing houses or payroll providers, employment agencies (where your employment with us involves using these services)
- Insurance brokers and insurers and related third parties, e.g. lawyers and loss adjustors for the purpose of risk mitigation, securing insurance cover, maintaining and administering that cover and processing any claims that may arise as a result.
- Recognised Teaching Centres, where images or voices are shared in a recording of teaching activities
- Your family, associates and representatives
- Current, past or prospective employers
- Healthcare, social and welfare organisations
- Suppliers and service providers
- Auditors
- Local and central government
- Consultants and professional advisors
- Trade union and staff associations
- Survey and research organisations
- Funders and sponsors

Some information about staff is also sent in coded and anonymised form to the Higher Education Statistics Agency (HESA). HESA's privacy notice is available here: [Privacy information | HESA](#)

6. Transfer of personal data outside the UK

Your data may be transferred outside the UK. Third party providers who deliver our services, such as externally hosted software or cloud providers, may store or transfer personal data we share with them outside the UK. When we transfer your personal data outside the UK we protect it by ensuring that those transfers are made in compliance with data protection laws. Generally this means that we put in place a contract with the third party that includes the standard international data transfer contractual terms approved by the ICO. You can get further information about this by contacting us.

7. How do we protect your data?

We take the security of your data seriously. Details on university wide measures surrounding IT security can be found in the University's IT Security Policy which sets out the definition of commitment to and requirements of Information Technology and Security. It specifies regulations to be implemented to secure information and technology that the University manages and to protect against the consequences of breaches of confidentiality, failures of integrity and interruption of availability.

We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the performance of their duties.

Where we engage third parties to process personal data on our behalf, they do so on the basis of written instructions contained within a contract, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

8. What are your rights in relation to your personal data?

As an individual whose data we process, you have certain rights in relation to your personal data. You can find detailed information about your rights in our [Guide to data protection rights](#) and while it is intended for students, the rights outlined in the document also relate to staff.

You have the right to:

1. Access personal data held by us about you, and to ask us to confirm that your personal data is being processed by the University of London
2. Withdraw your consent for us to process your personal data where we have relied on that consent as our legal basis.
3. Request that we rectify any inaccuracies where the data we hold about you is inaccurate or incomplete. Please be aware that we may need to verify the accuracy of new data you provide to us.
4. Have your data erased by us, where there is no good reason for us to continue to process it. We may not always be able to comply with your request of erasure for legal reasons which will be explained to you if they apply when we respond to your request. The circumstances where this applies can be found in the [guide to data protection rights](#).
5. Restrict the processing of your personal data in certain ways, for example if you dispute the accuracy of the personal data held by us.
6. Obtain personal data you have provided to us in a structured, commonly used and machine readable format for reuse.

7. Object to certain processing of your personal data where we are relying on a legitimate interest but you feel it impacts on your fundamental rights and freedoms. Please be aware that we will review our processing of your data but we may demonstrate that we have compelling legitimate grounds to process your data which override your rights and freedoms.
8. Ask us not to use computers to make decisions about you and ask us to stop doing so.

If you would like to exercise any of your rights please look at the information available on the [data protection webpage](#)

9. Who do I contact with questions?

If you have any questions or concerns about the way the University of London handles your personal data which have not been answered by this privacy notice, please email the [Data Protection team](#)

You may find the answer to your question on the [data protection webpage](#)

If you are still unsatisfied with the information you have about our handling of your personal data, you have the right to lodge a complaint with the data protection authority in your country or our main data protection regulator, [the Information Commissioner's Office](#).