



Staff Privacy Notice

Introduction

This privacy notice is relevant to current and former staff of the University, including full-time and part-time permanent and fixed-term employees in clerical, technical, administrative, professional and academic roles, freelancers, independent contractors, consultants and 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. Suzie Mereweather is our Data Protection Officer and you can contact her 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.

What information do we collect from you?

During the course of your time working for us and or with us, we will collect, obtain and hold a range of data about you that may be able to identify you directly or indirectly. If and when you cease to be employed or engaged by us, we will continue to hold some data about you for a predefined period of time in order to fulfil our remaining tasks and obligations.

The personal data that the University holds about you as a member of staff will include 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.
- Dietary requirements

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 for pay and expenses purposes.

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.

Basic information about your activities in the University

Including use of information and communication systems, such as CCTV footage and access times from swipe card access, or an IP address if you access information from a device.

Special category data

The University may also process some kinds of more sensitive information about you that is classed as 'special category' data, and which receives additional protections under law, and in terms of our processing of it.

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

How do we collect this information?

Much of this data we will have asked you to provide to us directly when you started your employment.

Alternatively, we may have asked you for it during your employment, or you may have provided it to us independently in order for us to help you with something.

If we do not receive information directly from you, we either generate it ourselves (such as your employee ID and username), or we receive it from third parties, such as:

- HM Revenue and Customs (HMRC)
- Pensions scheme providers
- Disclosure and Barring Service
- Individuals or organisations that you named as a referee.
- Employment and other agencies

We request 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.

Why do we collect this information?

In order to be able to process your data lawfully, we must rely on a specific lawful basis, depending on the main reason why we need the data. Below we will explain these lawful bases and when they might be used.

Necessary for the University to comply with a legal obligation

We process data about you under this legal basis when we need to in order to comply with UK legislation, 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, disciplinaries and changes to your employment such as promotion, pay rises, location changes. These examples are not exhaustive.

Necessary for the purposes of the University's legitimate interests

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 UoL email account, and give you personalised access to buildings, IT applications, resources and network services such as Wi-Fi
- 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.
- 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 in order to protect your life or that of another person, for example in an emergency situation 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. 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 if, for example, wished to send you marketing, or to process your data where we cannot rely on one of the above bases.

Processing in the substantial public interest

For the purpose of securing insurance cover for the general protection of the University and its staff, maintaining and administering that cover and processing any claims that may arise as a result, which enables our staff to access the University of London's insurance whilst on approved business or field trips abroad.

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.

Special category data is defined as information which reveals:

- Your race or ethnicity, religious beliefs, sexual life or orientation, or your political opinions.
- A trade union membership.
- Information about your health, including:
 - Any medical condition, health, and sickness records
 - Occupational health referrals;
 - Where you leave employment and the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
 - Information required for medical physicians and / or pension providers; and

- Details of absences from work (other than holidays) including time on sick leave or statutory / family leave.

We are most likely to use this data for these legal bases:

- Processing is necessary for the establishment, exercise or defence of legal claims against the University.
- We have asked for and received your explicit consent to process your data for a specific purpose

We also use special category data in other situations. The legal bases that apply to each of these situations are:

Processing is necessary for us to carry out our obligations or exercise our (or your) rights under employment, social security and social protection law

This applies when we:

- Keep a record of reasonable adjustments for a disability to allow us to meet our obligations under the Equality Act
- Ensure that you are physically fit to work in a particular role
- Set up a voluntary salary deductions to a trade union

Processing is necessary for purposes of preventive or occupational medicine and to assess your working capacity as an employee

This applies when we obtain advice from medical professionals, such as occupational health or GPs, with regards to making adjustments to your working practices due to a health condition.

Processing is necessary 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.

Processing is necessary for statistical purposes

We use this when we collate and analyse data to improve our internal processes or to meet external initiatives such as Athena Swan. 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.

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.

The University has retention schedules on the [Records Management Intranet](#) which document for how long different information is required. As the retention schedules indicate, we need to keep different data for differing periods of time, and you will always be told how long your personal information will be kept, or how

we calculate this – this will either be when you give it to us, or if you don't give it to us yourself, as soon as possible after we obtain or receive it. We keep your personal data in accordance with the University's retention schedules

Some basic information about our former staff is transferred to the University Archives for permanent preservation so that it can be professionally managed in order to facilitate future historical research enquiries.

When it is no longer required in line with its retention period, personal information is securely and permanently destroyed.

Who do we share your information with?

Whilst 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, and the data is proportionate to the need. There is guidance and governance in place to help staff to ensure that only the necessary data is made available to other departments or third parties who would not otherwise have access to it.

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 internally

- 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

Third parties with whom information about staff may need to be shared by the University

- 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 court 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
- 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)
- 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.

In most cases, information about how your data is shared will be given to you closer to the time by the relevant department.

Data will be stored in a range of different places in HR management systems including third party platforms and on other IT systems (including email).

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.

What rights do you have in relation to the way we process your data?

As an individual whose data we process (a data subject), you have certain rights in relation to the processing. You can find detailed information about your rights as a data subject in this [location](#) and whilst it is intended for students, you may read it as applicable to staff also, in terms of the rights conferred onto data subjects.

You have the right to:

- Withdraw your consent for us to process your personal data where we have relied on that consent as our basis for processing your data.
- Ask us to confirm that your personal data is being processed and to gain access (i.e. have a copy) of that data as well as to be provided with supplemental information about the processing.
- Request that we rectify any inaccuracies where the data we hold on you is inaccurate or incomplete.
- Have your data erased by us, although in certain circumstances we may not be able to do this. The circumstances where this applies can be found in the [guide to data subject rights information](#).
- Restrict the processing of your personal data in certain ways.
- Obtain your personal data for reuse.
- Object to certain processing of your personal data.

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

Make a complaint

If you have any concerns about the way that we have handled your personal data please **email the Data Protection team** as we would like to have the opportunity to resolve your concerns.

If you're still unhappy, you have the right to **complain to the Information Commissioner's Office** (an independent body set up to advise on information rights for the UK) about the way in which we process your personal data.