# Logo  Description automatically generated

# **Colleague Privacy Notice**

This document sets out how The Open University collects and uses the [**personal data**](#_bookmark11) of its staff, volunteers, and anyone who works for or on behalf of The Open University.

This document will be updated from time to time in order to ensure compliance with data protection legislation. It supersedes the Staff, Workers and Applicants privacy notice

##  Scope

This document applies to

* All members of staff in the[**Open University Group**](#Glossary_2)
* All workers, including but not limited to script markers and invigilators, etc.
* Partner and contractor staff who work closely with OU staff and have OU computer usernames, including agency staff, self-employed consultants, freelancers,
* Volunteers, emeritus professors, and visiting academics.
* OUSA staff where we provide payroll and IT services

This document does not apply to

* Research students – see **Student** privacy notice
* Corporate contacts who do not have access to OU data or systems – for business contacts, clients and suppliers, please see the corporate contact privacy notice at [www.open.ac.uk/privacy](http://www.open.ac.uk/privacy)
* Job applicants – please see the [Recruitment and Selection](https://about.open.ac.uk/sites/about.open.ac.uk/files/files/recruitment-selection-privacy-notice.pdf) privacy notice

For more information, see [www.open.ac.uk/privacy](http://www.open.ac.uk/privacy)

##  Policy

### **Who we are**

 The Open University is the [**data controller**](#_bookmark11) in relation to the processing activities described below.

Where this policy refers to “we”, “our” or “us” below, unless it mentions otherwise, it is referring to The Open University and organisations in the [**Open University Group.**](#Glossary_2)

If you have any questions about our use of your personal information, or wish to exercise your rights, please contact the Information Rights Team:

* + - Email: data-protection@open.ac.uk
		- Telephone: +44(0)1908 653994
		- By post: The Data Protection Officer, PO Box 497, The Open University, Walton Hall, Milton Keynes MK7 6AT

### **What information do we collect about you and how do we collect it?**

We hold a range of information relating to our colleagues to enable us to manage staff contracts, fulfil our obligations, and run the business effectively. Depending on your relationship with the OU, this can include the following:

**Information you provide or create:**

* Personal details such as name, date of birth, gender, marital status, contact details and emergency contact details
* Application and engagement information (see the recruitment and selection privacy notice) including work and employment history, right to work details, criminal convictions. For volunteers, this may include volunteering history, subject specialism and current employment
* Requests for contract changes, including agile working requests and supporting documentation
* Salary payment details, including bank details and national insurance number, and salary sacrifice and direct payment information, including trade union membership if relevant.
* Equality monitoring data
* Training records, participation and completion of online training, and professional membership(s)
* Performance evaluation records
* Details of queries about staffing as it relates to you, and related correspondence.
* Information relating to sickness, leave and absence, and details of casework including parental leave, disciplinary, grievances, etc. including any compensation payments
* Expenses claims and payments
* Copy of driving licence and motor insurance
* Recording of all calls made by or received by front line staff dealing with enquiries, i.e. the IT helpdesk, Computing helpdesk, People Services staff, and calls made to the main OU phone number
* Learning event or meeting recordings, which capture some personal data of participants.
* Health and safety information, including accident reports.
* Business travel information, including information provided for travel overseas, where relevant.
* Work allocation, workload and work monitoring, working hours and attendance
* Photos
* Work correspondence and documentation relating to you

**Information we create or collect automatically**

* Workplace location and contact details, including telephone numbers, email address
* Salary, payroll, pension and benefits information
* CCTV and ANPR images. There are number plate recognition cameras at campus entry and exit, but these are not linked to databases containing vehicle information.
* Network user account information and network, IT systems, communications and internet usage history
* Swipecard door entry records

**We may receive some information about you from third parties:**

* References about you from current or previous employers or other relevant people
* For certain roles, we will request information from the Disclosure and Barring Service (DBS) or another service provider regarding advanced security screening.
* Recommendations received from the “Access to work” scheme regarding adjustments to support disabled people at work.
* Information from our occupational health provider, which is provided to your line manager and People Services.

### **Our lawful bases for using your data**

Processing your personal information is necessary for us

* + - to perform our contract or agreement that we have with you
		- to allow us to meet our legal obligations, or
		- to enable us to pursue our legitimate interests to run the business.

### **How do we use your data?**

4.1 Our activities include the following:

Contract administration and support

* + - Maintaining your engagement record and work history, including changes of circumstances, work patterns etc. In certain circumstances you may provide sensitive data in order to support an agile working request or other enquiry. This would be done with your explicit consent to use the data for that request only.
		- We ask for information about criminal convictions and offences on recruitment, and carry out DBS checks for certain roles. Our condition for processing this data is that it is necessary for our employment obligations and safeguarding the rights of our staff (health and safety legislation), that it's in the public interest for safeguarding our students, and that it is necessary for the prevention of crime and protecting the public against dishonesty (depending on the role and conviction).
		- Managing requests for leave, including special leave and parental leave
		- Deciding on continued engagement, or promotions, which may include requesting information from external referees.
		- Paying you and providing other agreed benefits including statutory sick pay, deducting tax and National Insurance. Our lawful basis for processing any details about your trade union membership (where relevant) for the purposes of processing union fee salary deductions is your explicit consent. Where we process information about your participation in strike action, this is necessary for your contract with us in order to pay you correctly.
		- Pension administration
		- Performance management and reporting
		- Providing and recording personal development and training
		- Conducting grievance or disciplinary processes, or handling legal disputes and claims. If you provide “[special category](#_bookmark11)” information for this purpose, it will not be used for any other purposes. Our lawful basis for this processing of special category data is that it is necessary in relation to our obligations under employment law, or is necessary for the establishment, exercise or defence of legal claims.
		- Processing expenses claims or to book work-related travel or accommodation. Our travel booking provider keeps details of prescription medication and health conditions to help resolve difficulties when travelling on OU business Lawful basis
		- Managing the termination of our working relationship
		- Managing sickness absence, providing occupational health and wellbeing support services, and assessing fitness to work

Our lawful basis for processing **Special category** data about your health in relation to managing sickness absence, providing occupational health services, and assessing fitness to work is that it is necessary to comply with our obligations under employment law

If you use the employee assistance programme, then the lawful basis for you to provide your personal data to our supplier, which is an independent data controller, would be explicit consent

Our lawful basis for processing **special category** data you provide about reasonable adjustments under the Equality Act 2010 is that it is necessary to comply with our legal obligations under the Act, and the condition for processing the special category data relates to our employment obligations and safeguarding your fundamental rights.

If you provide information about an adjustment you need which does not relate to a disability, then the lawful basis and condition for this would be explicit consent

Conduct of your role

* + - Correspondence and files associated with you will be used for work purposes by relevant internal and external colleagues.
		- Providing communications about University news and events (which are not necessarily directly related to your employment)
		- staff data may be collected as part of the management of student queries, requests or administration. This is necessary to keep an accurate record of communications with students and to enable the university to fulfil its safeguarding responsibilities.

Management information, planning and service improvement

* + - Analysing workforce data for workforce planning, improving staff retention, experience and staff development
		- Equal opportunities monitoring. The lawful basis for processing [**special category**](#Glossary_2) equality monitoring data is that it is necessary for reasons of substantial public interest, specifically monitoring equality of opportunity or treatment
		- Provision of references on your request to your potential employer
		- Managing the business, accounting and audit activities
		- Planning, assessing, improving and reporting on business activities
		- We record telephone calls made or received by individuals logged into the Aspect system, for staff training purposes
		- Requesting participation in surveys to help us plan and improve our services and systems
		- Producing statistical information for publication
		- Benchmarking our activities against other organisations
		- Analysing and improving use of our websites and systems through using cookies and similar technologies

Systems provision and maintenance

* + - Providing and monitoring network and ICT systems, and IT assets and equipment, and ensuring network and information security
		- Testing and maintaining our systems and to ensure robust performance

Providing a safe environment and to prevent and detect crime

* + - Administration of The Open University’s CCTV system, to provide a safe environment and facilitate the prevention and detection of crime
		- Vehicle registrations are used, if provided to the OU, to manage car parking and security
		- To prevent fraud and other criminal activities, for example fraud in relation to public funding
		- To identify users of library resources who have breached our subscription terms by downloading excessive material
		- To monitor use of IT services and ensure network and information security

Business continuity

* Maintaining contact details for emergency planning and emergency situations

Managing legal claims

* Managing employer insurance claims, legal advice, debt collection and similar cases

Externally funded bids

* Costing bids for externally funded projects etc., and to provide information to funders, lead institutions and auditors

Compliance

* We may wish to comply with overseas tax legislation. Names, salaries, addresses and/ or identity documents of specific members of staff may be required by overseas tax authorities.
* We record concerns about people being drawn into terrorism (Prevent)
* Undertaking Subject Access requests and Freedom of Information requests. We may conduct central searches of OU systems in order to respond to these queries. If information about you or associated with you is retrieved and could be disclosed, you will be informed and may be consulted about disclosure. Information about people who are not the subject of the request will generally be redacted.

Academic research

* Personal data may be processed for academic research purposes on the basis that this is in the public interest, and the results of the research will not lead to decision- making about an individual or groups of individuals. Your personal data will be captured if you facilitate recordings of learning events etc. to be made available to students; and if you take part in business meetings which are recorded. Informal meetings may be recorded for the purpose of notetaking and once the notes have been written up, the recording will be deleted.

 If you do not provide some of the information we need, it may put your engagement with us at risk.

### **Automated decision making**

Automated decision-making means making decisions about you using no human involvement e.g. using computer modules or calculations to identify specific staff to take actions on, or to identify the actions to take relating to a member of staff, and carrying out those actions.

We do not make staff management decisions based on automated decision-making.

### **Who do we share your information with?**

 We share data with a number of organisations for specific purposes.

|  |  |  |
| --- | --- | --- |
| **Disclosure to** | **Details** | **Basis for transfer** |
| Higher Education statistics Agency (HESA), part of JISC | Some information will be sent to the HESA (part of JISC) for statistical analysis and to allow government agencies to carry out their statutory functions. You are advised to refer to the[HESA staff collection notice](https://www.hesa.ac.uk/about/regulation/data-protection/notices) for further details | Public task |
| Home Office, UKVisas and Immigration | In order to fulfil the University's obligations as a visa sponsor | Legal obligation |
| Security screening organisations, e.g.the Disclosure and Barring Service | Required for certain sensitive posts to assess applicant's suitability for positions of trust. See [Policy](http://www.open.ac.uk/foi/main/sites/www.open.ac.uk.foi.main/files/files/ecms/human-resources/c/criminal-record-checks/Recruitment-of-Ex-Offenders-Policy-HRP031.pdf) [on the recruitment of ex offen](http://www.open.ac.uk/foi/main/sites/www.open.ac.uk.foi.main/files/files/ecms/human-resources/c/criminal-record-checks/Recruitment-of-Ex-Offenders-Policy-HRP031.pdf)ders | Legitimate interest; (employment andsocial protection legislation) |
| National Funding bodies, e.g.HEFCE, HEFCW | Data submitted for the Research Excellence Framework (REF), and potentially the TeachingExcellence Framework (TEF) | Public task |
| Funding bodies | Names and details of expenditure, i.e., salary levels, employment contracts, to ensure compliance withfunding contract. | Contracts with funding bodies forparticular projects |
| Provision of CVs to identify the kind of individual who may be employed on a research project, as part of a bid | Legitimate interest in successfully bidding |
| Prospective employers | References will be provided on request, stating role, dates of engagement and suitability for the role – see reference policy |  |
| External referees for academic promotions | Provision of CVs for individuals being considered for academic staff promotion, for reference purposes and feedback | Legitimate interest of ensuring progression ofrelevant staff |
| External research organisation/ universities | Where an individual role requires study, work, or a placement at another organisation it may be necessary for the University to transfer personal data to the external university or employer, whether this is within the UK or abroad. This may require some data being sent outside the EEA. | Contract |
| Partner Universities for Research Projects | Where collaboration with another institution is required, it may be necessary for the University to transfer personal data such as salary details, for the purposes of preparing a bid for a grant. This may require some data being sent outside the EEA. | Contract |
| Mortgage lender and letting agencies | In order to allow these organisations to verify employment for mortgages and tenancy agreements. | Consent |
| HM Revenues & Customs (HMRC) | Real Time Information released to HM Revenue & Customs (HMRC) in order to collect Income Tax andNational Insurance contributions (NICs) from employees. | Legal obligation |
| Universities SuperannuationScheme (USS) | Data required for the provision of pensions by these providers. | Legal obligation |
| Overseas tax authorities | Data about e.g. high earning staff salary details required by overseas tax authorities to approve tax exemption or other benefits | Legitimate interest in being tax exempt |
| Students | Associate Lecturer name and contact details are made available to students allocated to them. Associate Lecturers’ names, email addresses and work telephone numbers are released to students who book a place at a Learning Event at which the Associate Lecturers are working.External examiner names and reports are madeavailable to students in line with QAA guidance | Contract |
| Event Venues or providers | Details of staff working, or attending, an event on behalf of the University may have their details shared with the host venue and/ or event provider for contact purposes and/or to enable reasonable adjustments to be accommodated. | Contract |
| Organisations conducting salary benchmarking | Pay data is shared to enable the effective benchmarking of pay and benefits. This may include Job titles but not individual names | Legitimate interest in ensuring our pay is comparable withinthe sector |
| Trade Unions | Some personal information may be sent to the trade union to facilitate and assist with collective bargaining and negotiations. Personal information may also be sent to the trade union to enable the University to carry out any collective consultation exercises. | Legal obligation and legitimate interest |

Names and contact details of staff working on partnerships and directly with other organisations, with members of the public, or with students, are likely to be shared with relevant people where necessary. This is in order to facilitate their work, and forms part of their contract of work, if directly engaged by the OU.

Academic staff may put certain information in the public domain, in order to fulfil funder requirements, and to build their academic profile. For example, their ORCID (unique ID), their publications, and contact details.

Where necessary, we will also share information when required to by law or in the public interest, with, for example, the police or HM Revenue and Customs, or to exercise or defend our legal rights.

### **Third party suppliers and service providers**

We use third party suppliers and service providers for a number of activities, from IT services and library systems authentication, to providing staff development and occupational health services, and requesting expert advice. We engage consultants for specific pieces of work, which may involve them processing personal data on our behalf. We may also provide staff details to our insurers or legal consultants, external auditors, or debt collection agencies.

It is in our legitimate interest to use third party suppliers to maintain cost effective and efficient operations, and it may be necessary for our contract with you, to share data with third parties.

When we use third party service providers, we only disclose to them any personal information that is necessary for them to provide their service. We have a contract in place that requires them to keep your information secure and not to use it other than in accordance with our specific instructions.

###  **Other ways we may share your personal information**

We may transfer your personal information to a successor organisation if The Open University ceases to exist. We may also transfer your personal information if we are under a duty to disclose or share it in order to comply with any legal obligation, to detect or report a crime, to enforce or apply the terms of our contracts or to protect the rights, property or safety of our staff, students and visitors. However, we will always aim to ensure that your privacy rights continue to be protected.

### **Do we transfer information outside the European Economic Area (EEA)?**

Generally, information you provide to us is stored on our secure servers, or on our cloud-based systems which are located within the EEA.

However, there are times when we do need to store information outside the EEA. If we transfer your information outside the EEA, we will take steps to ensure that appropriate security measures are taken to protect your privacy rights as outlined in this policy. Generally we impose contractual obligations on the recipient of your personal information, i.e. EU international [standard contractual clauses](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) with the [UK addendum](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/). We may ensure that the recipients are subscribed to international frameworks that ensure adequate protection, e.g. the [US data privacy framework.](https://www.dataprivacyframework.gov/s/) Occasionally we may ask for your consent to share data outside the EEA.

If you are supporting students outside the EEA, it may be necessary for some of your personal information to be transferred to countries outside the EEA, and for institutions which have a partnership arrangement with the University to have access to it. Such transfers are necessary for the performance of your contract, and we have appropriate contracts in place with partner organisations to safeguard your data.

### **How long do we keep your personal information for?**

If we collect your personal information, the length of time we keep it for is determined by a number of factors including our purpose for using the information and our legal obligations and regulatory requirements.

We have a retention schedule for information and keep identifiable records only for as long as they have a legal or business purpose.

Generally, staff data will be kept for 6 years after engagement ends, with some information being deleted sooner. However, we keep summary records of staff and pension information in the long term. Some health and safety and occupational health data will be kept for 40 years as these may have a long-term liability.

See the retention schedule for more information (available internally).

###  **Your rights**

You have a number of rights in relation to your personal information, which apply in certain circumstances. In order to exercise any of these rights, please contact us using the details in Section 1 of this document.

You have the right to:

* + - [access the personal information](https://ico.org.uk/your-data-matters/your-right-of-access/) that we hold about you.
		- [correct inaccuracies](https://ico.org.uk/your-data-matters/your-right-to-get-your-data-corrected/) in the personal information that we hold about you.

In certain circumstances, you have the right

* + - to [have your data deleted](https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/) when it is no longer required
		- to [limit how we use](https://ico.org.uk/your-data-matters/your-right-to-limit-how-organisations-use-your-data/) your personal information
		- obtain a copy of your personal data in a structured electronic data file ([data portability](https://ico.org.uk/your-data-matters/your-right-to-data-portability/))
		- [object to the use](https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-your-data/) of your personal data

You also have rights relating to automated decision making, where in certain circumstances you have the right to not be subject to automated decision making, and can request human intervention.

In the rare situations where we rely on consent as the legal basis on which we process your personal information, you may also withdraw that consent at any time by contacting the team you provided the personal data to, with the details of your request.

If you are concerned about the way we have processed your personal information, you can complain to the Information Commissioner’s Office (ICO). Please visit the [ICO’s website](http://www.ico.org.uk/) for further details, or you can use their online tool for reporting concerns: <https://ico.org.uk/concerns/>

##  Glossary

#### Personal data

According to the General Data Protection Regulation, ‘personal data’ means 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.

#### Data Controller

A data controller determines the purposes for which and the manner in which any personal data are processed. In essence, this means that the data controller decides how and why personal data are processed.

#### Special categories of data

The General Data Protection Regulation sets out “special categories” of data which have to be given additional protection. These comprise your racial or ethnic origin, religious beliefs, political opinions, trade union membership, genetics, biometrics (where used for ID purposes) physical or mental health, sex life and sexual orientation. Information about criminal offences or criminal proceedings are treated similarly.

**Cookies**

A cookie is a small amount of data, which often includes a unique identifier that is sent to your computer or mobile phone browser from a website’s computer and is stored on your computer’s or mobile phone’s hard drive. Each website can send its own cookie to your browser if your browser’s preferences allow it, which the site can then access when you visit it again to track online traffic flows, for example. A website cannot access cookies sent by other websites.

**The Open University Group**

For the purposes of this document, this refers to Open University WorldWide (OUW), Oen University Budget Accounts (OUSBA) but not Open College of the Arts (OCA).

**HESA Information**

Equality information requested at application or final offer stage, to provide to the Higher Education Statistics Agency on behalf of the Office for Students:: Birthdate, Activity or Employment Before OU, Higher Education Provider, Worked At Before OU, Highest Qualification Held, Academic Teaching Qualification 1-6, Academic Discipline Working in at OU 1-5.