Colleague Privacy Notice

This document is relevant to staff, workers, job applicants, contractors, agency staff, volunteers and anyone who works with or on behalf of the Open University

Contents

Summary

The Open University needs to collect and process personal data in order to carry out our duties as an employer, partner, or customer.

This document sets out how we use your personal data.

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.

Version number: 1.0	Approved by: People Services, Information Rights Team
Effective from: December 2020	Date for review: December 2021

Scope

What this document covers

This document applies to

- All members of staff including, but not limited to, Associate Lecturers, and Open University Worldwide (OUW) staff.
- Job applicants
- 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 and Mulberry Bear nursery staff where we provide payroll and IT services

This document does not apply to

- Research students – see supplementary **postgraduate research 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

For more information, see also our Privacy and Cookies page

Policy

1. Who we are

1.1 The Open University is the data controller in relation to the processing activities described below. This means that The Open University decides why and how your personal information is processed.

Where this policy refers to "we", "our" or "us" below, unless it mentions otherwise, it is referring to The Open University.

The main establishment of the Open University is in the UK. If your data is collected by our office in the Republic of Ireland, then this will also be processed in the UK.

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.
- Data subjects within the EU can contact the Data Protection Officer c/o the Open University in Ireland: Holbrook House, Holles Street off Merrion Square, North Dublin 2, D02 EY84.

2. What information do we collect about you and how do we collect it?

2.1 We hold a range of information relating to our colleagues to permit us to run the business effectively. Depending on your relationship with the OU, this includes:

- Personal details such as name, date of birth, gender, marital status, contact details and emergency contact details
- Workplace location and contact details, including telephone numbers, email address
- National Insurance number, bank or building society details, payroll records and tax information
- Salary, annual leave, pension and benefits information
- Expenses claims and payments
- Copy of driving licence and motor insurance
- Recruitment or engagement records such as your CV, application, interview documents, references.
- Right-to-work documents/ migrant status
- Education, qualification and previous employment information including start date, posts held, previous salary. For volunteers, this may include volunteering history, subject specialism and current employment
- 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 you submit relating to sickness, leave and absence, and details of casework including parental leave, disciplinary, grievances, etc. including any compensation payments
- 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. Work allocation, workload and work monitoring, working hours and attendance
- Photos and CCTV 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
- Swipe card records

2.2 Where necessary, we may hold more sensitive information about you, called “special category” personal data, including:

- Information about your race or ethnicity, religious beliefs and sexual orientation (if you provide these) for the purposes of equality monitoring and fulfilling our duties under the Equality Act;

- Details about your trade union membership (where relevant) for the purposes of processing union fee salary deductions and liaison with trade unions;
- Information about your health for purposes of managing sickness absence, providing occupational health services and making reasonable adjustments
- Our travel booking provider keeps details of prescription medication and health conditions to help resolve difficulties when travelling on OU business
- Biometric data (such as fingerprint recognition systems) for security processes
- You may provide sensitive data in relation to an agile working request or other enquiry
- Information you provide on your application about any relevant criminal convictions
- Where appropriate, information about criminal convictions and offences for authorised background checks, using information from the appropriate statutory bodies (Disclosure and Barring Service for England and Wales, Disclosure Scotland, or Access NI in Northern Ireland).

2.3 We may receive some information about you from third parties

- Personal data may be provided by your employer organisation
- References about you from current or previous employers or other relevant people
- Recommendations received from the "Access to work" scheme regarding adjustments to support disabled people at work.
- We will receive information about you from our occupational health provider, which is provided to your line manager and People Services.
- For certain roles, we will request information from the Disclosure and Barring Service (DBS) or another service provider regarding advanced security screening.

---

3. How do we use your personal information?

3.1 Processing your personal information is necessary for us

- to perform our contract of employment with you (if we have one),
- to allow us to meet our legal obligations, or
- to enable us to pursue our legitimate interests to run the business.

3.2 These activities may include the following, depending on your relationship with us:

- Deciding on recruitment and appointment of staff, volunteers and contractors and checking legal entitlement to work in the UK.
    - It is possible that publicly accessible social media profiles will be viewed as part of the recruitment process. If so, applicants should be informed in the recruitment process.
    - Information you give about criminal convictions will be used to assess your suitability for a role.
    - If you are unsuccessful in applying for a role, your application form or CV may be shared with other business units to consider you for similar roles that are being recruited for.
- Maintaining your engagement record and work history, including changes of circumstances, work patterns etc

- 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
- Deducting tax and National Insurance
- Pension administration
- Performance management and reporting
- Conducting grievance or disciplinary processes, or handling legal disputes and claims. If you provide "special category" information for this purpose, it will not be used for any other purposes.
- Personal development and training
- Assessing fitness to work and managing sickness absence
- Providing wellbeing and support services, and occupational health and making reasonable adaptations to support you in the workplace
- Analysing workforce data for workforce planning, improving staff retention and staff development
- Equal opportunities monitoring
- 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
- Managing the termination of our working relationship
- Provision of references on your request to your potential employer
- 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.
- Correspondence and files associated with you will be used for work purposes by colleagues.
- 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.
- Managing the business, accounting and audit activities
- Planning, assessing, improving and reporting on business activities
- 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
- To help us improve our services via staff training. We record telephone calls made or received by individuals logged into the Aspect system, for staff training purposes

- We carry out activities to provide a safe environment, maintain security, and 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
- We carry out some activities manage our operations effectively
    - We log OU assets and equipment provided to you o We test and maintain our systems to ensure robust performance
- Managing our relationship with our suppliers
- Maintaining contact details for emergency planning and emergency situations
- Producing statistical information for publication
- Benchmarking our activities against other organisations
- Requesting participation in surveys to help us plan and improve our services and systems
- Managing employer insurance claims, legal advice, debt collection and similar cases
- 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.
- Costing bids for research projects etc., and to provide information to funders, lead institutions and auditors
- Providing communications about University news and events (which are not necessarily directly related to your employment)
- Analysing and improving use of our websites and systems through using cookies and similar technologies

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

Consent

3.4 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.

Profiling and automated decision making

3.5 We will use automated profiling of staff information for workforce and succession planning and for absence management processes – identifying patterns of sickness absence which will trigger an intervention under our attendance management procedures (Bradford scoring).

4. Who do we share your information with?

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

Disclosure to	Details	Basis for transfer
Higher Education statistics Agency (HESA)	Some information will be sent to the HESA 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 for further details	Legal obligation
Home Office, UK Visas 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 on the recruitment of ex offenders	Legitimate interest; (employment and social protection legislation)
National Funding bodies, e.g. HEFCE, HEFCW	Data submitted for the Research Excellence Framework (REF), and potentially the Teaching Excellence Framework (TEF)	Public task
Research funding bodies	Names and details of expenditure, i.e. salary levels, employment contracts, to ensure compliance with funding contract.	Public task
	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 and auditing use of funds.
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 of relevant 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 and National Insurance contributions (NICs) from employees.	Legal obligation
Universities Superannuation Scheme (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 made available 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 within the 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

4.2 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.

4.3 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

4.4 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.

4.5 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

4.6 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

4.7 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.

5. Do we transfer information outside the European Economic Area (EEA)?

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

5.3 If you are supporting students outside the UK, it may be necessary for some of your personal information to be transferred to international institutions which have a partnership arrangement with the University

5.4 Where we use service providers outside the UK, or we transfer data to international partners, we use appropriate contractual safeguards, for example the standard contractual clauses for international transfers. Occasionally we may ask for your consent to share data outside the EEA.

5.5 The main establishment of the Open University is in the UK. If your data is collected by our office in the Republic of Ireland, then this will also be processed in the UK.

6. How long do we keep your personal information for?

6.1 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.

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

6.3 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).

Unsuccessful applicant data will be retained for 12 months folllowing the recruitment process, apart from Associate Lecturer applications which are retained for 12 to 36 months.

---

7. Your rights

7.1 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.

7.2 You have the right to:

- access the personal information that we hold about you
- correct inaccuracies in the personal information that we hold about you

In certain circumstances, you have the right

- to have your data deleted when it is no longer required
- to limit how we use your personal information
- obtain a copy of your personal data in a structured electronic data file (data portability)
- object to the use 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.

7.3 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 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.

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.

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.