Staff, workers and applicants Privacy Notice

Contents

Summary

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

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.

Version number: 1.0	Approved by: Data Protection Officer
Effective from: 21st March 2018	Date for review: September 2018

Scope

What this document covers

This document applies to

- All members of staff including, but not limited to, Associate Lecturers, OUW and OUSBA staff.
- Job applicants
- All workers, including but not limited to script markers and invigilators, etc

This document does not apply to

- Research students – see supplementary **postgraduate research student** privacy notice
- OUSA staff , mulberry bear staff, futurelearn staff
- Other individuals carrying out activities on behalf of or with the OU: Agency staff, self employed consultants, freelancers, visiting academics, emeritus professors, staff of partner organisation or contractors – see the **visitor** privacy notice

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.

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

2.1 We create a record for you when you apply for engagement with us, or you start to work with us. Information will be held by Human Resources, by individual departments and by your line manager.

Information that you give to us

2.2 You will normally give us your personal details during the recruitment process, and information will be added to your record during the course of your engagement with the OU. Data we hold on you may include:

- Personal details such as name, date of birth, gender, contact and next of kin details
- National Insurance number, bank or building society details,
- Education, qualification and previous employment information, and right to work documentation.
- 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, grievances, etc.
- Health and safety information, including accident reports.
- We ask for your nationality, religion, sexual orientation, ethnic origin and disability information, but you can choose not to disclose this.
- We may ask for information about any unspent criminal convictions when you apply for a job.
- We may ask you to provide information to enable us to make any reasonable adjustments that you require
- We also conduct staff surveys, asking for your opinion on working at the OU.

Information that we create or collect

2.3 During your engagement with us, we may create or collect information which includes

- Contracts or terms and conditions of engagement and employment history,
- Pay and deduction details, superannuation details
- Sickness and absence records
- Health and safety records
- Workload or work allocation, working hours, attendance
- Performance management information, disciplinary records, investigations and casefiles
- Your photograph
- An email address which identifies your name

Information that we automatically collect

2.4 Some of our systems and processes automatically collect personal information. These include

- Door entry logging
- Work monitoring systems
- Participation and completion of online training
- Recording of all calls made by or received by staff logged into ASPECT.
- If learning events or meetings are recorded, then some personal data of participants may be automatically captured.
- IT system use is logged and monitored.
- CCTV cameras across OU sites. There are number plate recognition cameras at campus entry and exit, but these are not linked to databases containing vehicle information.

Information we receive from third parties

2.5 We may receive some information about you from third parties.

- References about you may be received from 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 Human Resources.
- 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 We collect and process a broad range of personal data about you in order to carry out our responsibilities as an employer, to manage our operations effectively, and to meet our legal requirements.

Recruitment activities

3.2 We collect your personal data on application forms and CVs etc. This is in our legitimate interest of managing recruitment processes, and identifying suitable candidates for recruitment.

- 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.

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

Activities relating to your contract with the OU

3.4 We use your personal data to carry out activities which are necessary for your engagement with the OU. These are likely to include the following:

3.5 Joining us

- Ensuring you are a suitable candidate if we have selected you for engagement. We will request information from previous employers and other cited as referees. For particular roles, we will request DBS checks, or enhanced security screening.
- Ensuring you have the right to work in the UK
- Providing you with an email address identifying you, which we will be used to contact you for work purposes, and enabling you to use it to carry out your role.
- Providing access to buildings and managing security. Your photograph is used on your ID card for identification and security.
- Providing access to relevant systems and services, such as IT systems and Library resources.

3.6 Through your engagement with us

- Payment of salaries and other payments
- Providing and managing training, development and progression

- Maintaining your engagement record and work history, including changes of circumstances, work patterns etc
- Managing requests for leave, including special leave and parental leave
- Monitor absence and sickness records in accordance with HR policy. Some information about your health will be required for sick pay and sick leave records.
- To review and manage your performance at work, and any disciplinary matters. If you provide "special category" information for this purpose, it will not be used for any other purposes.
- Managing complaints and grievances. If you provide "special category" information for this purpose, it will not be used for any other purposes.
- Enable attendance at work related events, including overseas travel where relevant, and the appropriate visa and passport requirements
- To assess suitability for promotion, which may include requesting information from external referees.
- Maintaining contact details for emergency planning and emergency situations
- Maintaining a safe environment and ensuring fitness to work
- Your personal data will be captured if you facilitate recordings of learning events etc, to be made available to students.
- If you give us information about your health or disabilities, we will refer you to our Occupational Health service for a recommendation. If relevant, we will provide reasonable adjustments for interviews, your work, and for attending events etc.

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

Activities carried out in our legitimate interest

3.8 We use personal data to plan, assess, improve and report on our activities

- Equality monitoring and statistics (which includes special category data, if you have given it to us, but is not used to make decisions about individuals)
- Work planning and management including recording time spent on different tasks, staff budget and forecasting
- Producing statistical information for publication
- Benchmarking our activities against other organsations
- Requesting participation in surveys to help us plan and improve our services and systems
- Costing bids for research projects etc, and to provide financial reports to funders, lead institutions and auditors
- We 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 monitor website usage in order to improve our service. For use of cookies on OU websites, please see www.open.ac.uk/privacy

3.9 We provide services to support staff and fulfill our obligations as an employer

- Provision of wellbeing and support services
- Providing communications about University news and events (which are not necessarily related to your employment)
- Provision of references on your request to your potential employer

- Travel services and activities to minimise disruption when travelling. Our travel booking provider keeps emergency contact details, details of prescription medication, health conditions to help resolve difficulties when travelling on OU business.

3.10 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 to ensure adherence to IT security policies or for statistical purposes, and ensure network and information security. We also monitor use of certain extremist websites so we can assess if there is a concern about peope being drawn into terrorism (*Prevent)*

3.11 We carry out some activities to manage our operations effectively

- We log OU assets and equipment provided to you
- We test and maintain our systems to ensure robust performance

3.12 We carry out activities to facilitate compliance and legal claims

- We audit our activities in order to ensure regulatory compliance
- We manage 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.
- We record concerns about people being drawn into terrorism (*Prevent)*

Activities we carry out as we have a legal obligation

3.13 personal data may be processed for academic research purposes on the basis that the results of the research will not lead to decision-making about an individual or groups of individuals. Where a researcher wishes to use sensitive personal data, such as ethnicity, explicit consent will be sought in advance from the individuals concerned

3.14 Compliance with legal obligations such as making external / statutory returns to HESA

- Undertaking subject access requests
- Tax management obligations (HMRC)
- UKVI right to work obligations, checking that any prospective employee can work in the UK

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
Disclosure and Barring Service (DBS)	Required for certain sensitive posts to assess applicant's suitability for positions of trust. See Policy on the recruitment of ex offencers	Legitimate interest; (employment and social protection legislation)
The Higher Education Funding Council for England (HEFCE)	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.	Contracts with funding bodies for particular 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 engagment and suitability for the role - see reference policy	
External referees for academic promotions	Provision of CVs for indviduals 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
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

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 are made available to students on request	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 or event provider for contact purposes and/or to enable reasonable adjustments to be accommodated.	Contract

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.

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

Third party suppliers and service providers

4.4 We use third party suppliers and service providers for a number of activities, from providing IT systems for file storage, 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.

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 EEA.

5.2 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. This would either be imposing contractual obligations on the recipient of your personal information, or ensuring that the recipients are subscribed to 'international frameworks' that aim to ensure adequate protection. For example, we would ensure that a supplier based in the USA has signed up to "Privacy Shield".

5.3 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.

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.

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 will 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.)

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 8 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 details removed from systems that we use to process your personal data

- restrict the processing of your personal data in certain ways
- obtain a copy of your personal data in a structured electronic data file
- object to certain processing of your personal data by us

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.

---

8. Contact us

8.1 Please direct any queries about this policy or about the way we process your personal information to our Data Protection Officer using the contact details below.

- 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.

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.

Privacy Shield
Privacy Shield is a framework which provides companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States. US based organisations self-certify to the Department of

Commerce and publicly commit to comply with the Framework's requirements, which is then enforceable under US law.

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.