Recruitment and Selection

Privacy Notice

This document sets out how The Open University collects and uses the personal data of anyone who creates a profile on our recruitment system, anyone who proceeds to make a job application and/or is offered a role with the Open University Group or Open University Students’ Association (OUSA).

This document will be updated from time to time in order to ensure compliance with data protection legislation.

The Open University needs to collect and process personal data in order to carry out our duties throughout the recruitment process.

Policy

1. Who we are

The Open University is the data controller in relation to the processing activities described below. For applicants to OUSA roles, OUSA and the Open University will be joint data controllers.

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.

If you have any questions about our use of your personal information, or wish to exercise your rights, please contact the Information Rights Team:
2. What information do we collect about you and how do we collect it?

We collect a range of information to permit us to manage the recruitment effectively, this includes:

- Information that you provide when you create a profile on our recruitment system. This includes your name, email address, country/region of residence.
- Your name, address and contact details, including email address and telephone numbers.
- Education, qualifications and previous employment information including start date, posts held, previous salary.
- Information about your eligibility to work in the UK.
- Recording of calls to the Resourcing Hub central number.
- CCTV images may be captured when visiting some OU locations. There are number plate recognition cameras at some campus entries and exits, but these are not linked to databases containing vehicle information.
- Information created and/or captured during your application and interview process.
We will also collect personal information about you from third parties, such as references supplied by former employers, background checks for example on qualifications, information from employment agencies, search consultants used during the recruitment process, and information from criminal records checks. The University will only seek information from third parties if you have given your permission for us to do so.

Where necessary, we will collect more sensitive information about you, called “special category” personal data, including:

- Equality information including information about your race or ethnicity, disability, religious beliefs and sexual orientation (if you provide these) for the purposes of equality monitoring and fulfilling our duties under the Equality Act.
- Information you give us about any reasonable adjustments you require, which may include the reasons for reasonable adjustments, disability or health information.
- 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).

This information is collected in a variety of ways, including from your candidate profile or CV, obtained from your passport or other identity documents, or from
notes taken at interview or from other forms of assessment such as online tests or practical exercises.

Your personal information will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

3. **Our lawful basis for using your personal data**

Processing your personal information is necessary for us to take steps before entering into an employment contract with you, or because it is in our legitimate interest.

The lawful basis for processing *special category equality monitoring data* you provide as part of your application is that equality monitoring is in our legitimate interest, and the condition for processing is that it’s necessary for reasons of substantial public interest, specifically monitoring equality of opportunity or treatment.

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.
We process information about applicant criminal convictions and offences. We rely on the processing conditions that it relates to 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).

We process biometric facial recognition data for online right to work checks. Our provider, Trust ID, uses a subcontractor to verify your identity using a face match score relating to a selfie you take and the identity documents you provide. See their privacy notice (IDology). Our lawful basis for doing this your explicit consent, and you can complete right to work checks in an alternative way if you choose.

4. How do we use your personal data?

We will use the information provided in your application to progress your application with a view to offering you an employment contract with us, and to fulfil legal or regulatory requirements if necessary.

We will use the contact details you give us to contact you to progress your application. We may also contact you to request your feedback about our recruitment process.

The information we ask for is used to assess your suitability for employment. You don’t have to provide what we ask for, but it may affect your application if you don’t.
We will use aggregated statistical information about recruitment in order to monitor and report on our business activities, and benchmark against other organisations.

For Open University Student Association (OUSA) roles we share the application information with OUSA.

4.1 Creating a profile and making an application
We will ask you to use our online application system or contact the recruitment team at resourcing-hub@open.ac.uk for an alternative.

We ask you for your personal details, and other questions relevant to the role. Our recruitment team and interview panel members will have access to this information.

You will be asked to provide equal opportunities information. This information won’t be made available to anyone outside the recruitment team, including any hiring managers, in a way which identifies you. The aggregated data is used for equal opportunities monitoring and reporting.

4.2. Shortlisting
Our hiring and recruitment teams shortlist applications for interview. If you have been notified that the recruitment is anonymous, they will not be provided with your name or contact details.

4.3. Interview and Assessments
We may ask you to attend an interview, and complete tests or assessments, or a combination of these. Information will be generated by you and by us, e.g., hiring managers assessing or making notes.
4.4. Offer
If we make a conditional offer of employment, we carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We must confirm the identity of our staff and their right to work in the United Kingdom and Republic of Ireland, and seek assurance as to their trustworthiness, integrity and reliability.

You must therefore provide:

- proof of your identity. Depending on the type of passport you hold, we may ask you to use our online identity verification service provider, or to provide documents in another way. Our online service will generate a face match score based on a selfie you take and the identity documents you provide. This counts as sensitive personal data. You can choose to provide documents in an alternative way.
- proof of your qualifications where appropriate.
- a criminal records declaration to declare any unspent convictions.
- We will carry out authorised background checks where appropriate We will contact your referees, using the details you provide in your application, directly to obtain references. We will also check employability of former OU employees.
- We will ask you to complete a questionnaire about your health to establish your fitness to work.
- We will ask you about any reasonable adjustments you may require under the Equality Act 2010. This information will be shared with relevant staff to ensure these are in place for when you start your employment.
- Sex, date of birth, bank details and national insurance number or equivalent – to process salary payments, tax and pension. You will be auto enrolled to the pension scheme but will be able to opt out.
- Emergency contact details – so we know who to contact in case you have an emergency at work.
- HESA information for our statutory and internal reporting where appropriate.

Information from your application will be transferred to your staff file and processed according to the colleague privacy notice.

5. Who do we share your information with?

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

<table>
<thead>
<tr>
<th>Disclosure to</th>
<th>Details</th>
<th>Basis for transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home Office, UK Visas and Immigration</strong></td>
<td>In order to fulfil the University’s obligations as a visa sponsor for non-UK nationals.</td>
<td>Legal obligation</td>
</tr>
<tr>
<td><strong>Security screening organisations, e.g. the Disclosure and Barring Service</strong></td>
<td>Required for certain sensitive posts to assess applicant’s suitability for positions of trust. See Safer recruitment and vetting policy</td>
<td>Legitimate interest; (employment and social protection legislation)</td>
</tr>
</tbody>
</table>

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.

5.2 Third party suppliers and service providers
We use third party suppliers and service providers for a number of recruitment related activities:

- IT systems
- Occupational health check provider
- Online identity verification system
- Text message provider
- Recruitment agencies
- Electronic contract signing provider.

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.

**5.3 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 disclose your personal information in order to report a crime, to comply with legal obligations or to enforce or apply the terms of our contracts or to protect the rights, property or safety of our staff, students and visitors.
6. **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. We generally impose contractual obligations on the recipient of your personal information, i.e. EU international [standard contractual clauses](#) with the [UK addendum](#). We may ensure that the recipients are subscribed to international frameworks that ensure adequate protection, e.g. the [US data privacy framework](#). Occasionally we may ask for your consent to share data outside the EEA.

7. **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.

Unsuccessful applicant data will be retained for 12 months following the recruitment process, apart from Associate Lecturer applications which are retained for 12 to 36 months. These retention periods are to allow for any recruitment queries, employment tribunals or other legal challenges.
Anonymous aggregated demographic data about applicants will be retained for a longer period for reporting purposes.

8. 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 below.

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
- 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.

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.
9. Automated decision-making

Automated decision-making means making decisions about you using no human involvement e.g. using automated models or calculations to identify eligible candidates.

We do not generally make recruiting or hiring decisions based solely on automated decision-making.

We may use automated decision-making to reach a decision about your application. This might be when we expect high numbers of applications as this helps us to efficiently, fairly and consistently identify candidates with the key skills and behaviours required for the role. Assessing applications is necessary for entry into a contract. The questions will have been assessed and agreed by our recruitment team for the optimum outcome.

Those that meet the minimum criteria required for the role will progress to the next stage of recruitment. The final decision on successful candidates will be reached by our hiring team following a consistent and rigorous non-automated selection process. If you have any concerns about your application progressing through an automated decision-making process, please contact the Resourcing-Hub@open.ac.uk.

10. Contact details

If you have any questions about our use of your personal information, or wish to exercise your rights, please contact the Information Rights Team:
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), Open University Student Budget Accounts (OUSBA) but not The 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.