Privacy Notice for Staff

Your Personal Data

The University of Glasgow *will be what is known as the 'Data Controller' of your personal data processed in relation to your employment relationship. This privacy notice explains how The University of Glasgow will process your personal data.*

Changes to this notice

The University may update this notice at any time and may also provide you with further more detailed notices on specific occasions where we collect and process personal data about you. Such additional privacy notices are supplemental to this main privacy notice. You should check this notice regularly to be aware of any changes. However, where any change affects your rights and interests, we will bring this to your attention and clearly explain what this means for you.

What we collect and why we need it

We are collecting your basic personal data such as

1. your name, address and contact details, including email address and telephone number, date of birth and gender;
2. the terms and conditions of your employment;
3. details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the University;
4. recruitment information including copies of right to work documentation, references, CV/resume, covering letter(s) and any other documents submitted as part of the application process, health declaration questionnaire and information completed by the employee prior to commencing employment;
5. information about your current and previous remuneration with the University, including entitlement to benefits such as pensions, salary sacrifice arrangements or insurance cover;
6. details of your bank account, national insurance number and tax status;
7. information about your marital status, next of kin, dependants and emergency contacts;
8. information about your nationality and entitlement to work in the UK;
9. information about your criminal record (where applicable);
10. details of your start date, schedule (days of work and working hours), hours worked and attendance at work;
11. information about your location and place of work;
12. employment records including job titles, work history, training records and professional memberships;
13. details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
14. details of any HR processes such as disciplinary, grievance or sickness absence procedures in which you have been involved, including any warnings issued to you and related correspondence;
15. assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;

16. information obtained through electronic means including, where applicable, swipe card access and computer logon information; and
17. Information about medical or health conditions, including whether or not you have a disability for which the University may make reasonable adjustments.

We may also collect, store and use the following “special categories” of more sensitive personal information:

1. equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religion or belief;
2. trade union membership;
3. information about your health, including any medical condition, health and sickness record;
4. Information about criminal convictions, offences and disclosure and barring.

The University collects this information in a variety of ways. For example, data is collected through applications, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of and/or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

The University collects personal data about you from third parties, such as references supplied by former employers (following consent), information from employment background check providers, and (if applicable) information related to criminal record checks and disclosure and barring.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

The University needs to process data to enter into an employment contract with you and to meet our obligations under your employment contract. For example, we need to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

The University needs to process data to ensure that it is complying with our legal obligations. For example, we are required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

Legal basis for processing your data

We must have a legal basis for processing all personal data.

All information detailed above is collected as part of our contract with the individual.

In other cases, the University has a legitimate interest in processing personal data before, during and after the end of the employment relationship. For example, processing employee data allows the University to:

1. run recruitment and promotion processes;
2. maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
3. operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;

4. operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
5. operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
6. obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet our obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
7. operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the University complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
8. ensure effective general HR and business administration;
9. provide references on request for current or former employees; and
10. respond to and defend against legal claims.
11. Data provided to appropriate College/School/Institute for Athena Swan purposes (details available on Athena Swan web site
12. Providing personal information to University Corporate systems (where appropriate) to co-ordinate corporate systems.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities – processing necessary for the purposes of preventative or occupational medicine).

We process other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. This is to carry out our obligations and exercise specific rights in relation to employment. Employees are entirely free to decide whether to provide such data and there are no consequences of failing to do so.

What we do with it and who we share it with

- Your information may be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, managers and business support administrators in the business area in which you work and staff support services staff e.g. IT, Occupational Health (where appropriate) if access to the data is necessary for performance of your role.

- We share your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks, where appropriate, from the Disclosure Scotland. Under the terms of agreement with the Home Office, access must be given for any compliance audits.

- We also share your data with third parties that process data on our behalf for the provision of benefits (Sodexo).

- The University will not transfer your data to countries outside the European Economic Area, with the exception of where your employee's employment with the University requires study, employment or a placement at another organisation it will be necessary for the University to transfer personal data to the external university or employer, whether this is within the UK or abroad. Employees should be aware that

some countries outside of the EEA have lower standards for the protection of personal data that those within the EEA.

The University takes the security of your data seriously. The University has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the performance of their duties e.g. IT security policy, encryption policy, all HR policies etc.

Where the University engages third parties to process personal data on our behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Registration with Information Services (IS) means that an employee's name, department/section, job title, email address and telephone number will appear in the University's electronic email and telephone directory which can be viewed on the internet. In exceptional circumstances employees can opt-out of the directory (in full or in part, such as declining contact details), either at the point of first registering with IS or later by contacting your Head of HR. Employees may also have their details on the relevant departmental web pages but can ask that these be removed or deleted.

The University routinely logs information about use of IT facilities for statistical purposes and to ensure effective systems operations. The University may also monitor electronic communications to ensure that they are being used in accordance with the University's Regulations for the Use of University ICT Systems and Facilities and, specifically, to prevent or detect crime.

Each employee is required to provide a digital image of themselves for reproduction on their University campus card, which will be used for the purpose of identification. The University may commission photography on campus or at specific events, such as award ceremonies, for use in its promotional material and employees may appear on the resulting images, which may be published.

Employee personal data (not including special categories) may be processed for academic research purposes (i.e. where there is only benefit to the researcher alone or the researcher and University combined) 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 special categories data, such as ethnicity or health, explicit consent will be sought beforehand from the individuals concerned.

Some of the reasons for processing your data overlap and there may be several grounds, which justify our use of your personal data.

The University may need to disclose the personal data of employees to organisations contracted to work on its behalf, which could include its pension providers, insurers or professional advisors such as lawyers or auditors and Uniforum. The University may also disclose data to external organisations undertaking market research or academic researchers provided no personal data is published. In certain circumstances the University passes the personal data of employee debtors to an external debt collection agency if the University has been unable to recover the debt by normal internal financial or HR processes.

The University has a statutory requirement to disclose employee personal data to the Higher Education Funding Council for England (HEFCE) and the Higher Education Statistics Agency (HESA) and/or their nominees/successors. The HESA return does not include any names of staff or contact details. The University may also disclose personal data to HEFCE and its partner bodies during the Research Excellence Framework (REF). The University

provides anonymised data to UCEA, XpertHR or appropriate HEIs for benchmarking purposes.

Data Sharing with Third Parties

On occasion the University may engage with a third party provider to facilitate your contract of employment or to meet a legal requirement or where we have another legitimate interest in doing so.

Third party service providers includes (but is not limited to) our pension providers, benefit providers and any other relevant service which the University may procure to a third party provider such as auditing and legal services. We may also share data with external interview panellists for recruitment and selection purposes.

The University requires any third parties to respect the security of your data and to treat it in accordance with the law. All third party service providers are required to enter into a formal data-sharing agreement with the University and must demonstrate that they have appropriate security, safeguards and policies in place to process your data.

The University will require that any third party storing your data do so securely with access limited to staff who have a requirement to access the data for reasonable and legitimate purposes.

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the University in whole or in part. We may also need to share your personal information with a regulator or to otherwise comply with the law.

How long do we keep it for?

We will hold your personal data for the duration of your employment plus 6 years following the end of your employment. We will, however keep a record of your employment at the University indefinitely for tax and pension reasons. See retention schedule.

How we use special categories data:

Special categories of personal information require higher levels of protection. We may process such data in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out any legal obligations.
3. Where it is needed in the substantial public interest,

Less commonly, we may process this information where it is needed in relation to legal claims, or where it is needed to protect your interests (and you are not capable of giving your consent) or where you have already made the information public.

In an HR context, we would anticipate use of special categories data in the following ways:

1. using information about your physical or mental health or disability status to ensure that you are fit for work, to ensure your health and safety in the workplace, to manage sickness absence, to administer benefits, and to consider any potential reasonable adjustments and support you if you have any health concerns. All health related information is stored securely, is only accessible by those with a legitimate interest to view that data such as Occupational Health, HR and your line manager and, if being sent in electronic format must be password protected;
2. information related to leaves of absence including sickness absence or family related leave, to comply with our legal obligations;

3. we will also use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual orientation, to ensure meaningful equal opportunity monitoring and reporting; and
4. we will use trade union membership information to pay trade union premiums and to comply with any relevant legal obligations.

What are your rights?

As a data subject, you have a number of rights. You can:

1. access and obtain a copy of your data on request;
2. require the University to change incorrect or incomplete data;
3. require the University to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
4. object to the processing of your data where the University is relying on our legitimate interests as the legal ground for processing.

If you wish to exercise any of these rights, please contact dp@gla.ac.uk.

*Please note that the ability to exercise these rights will vary and depend on the legal basis on which the processing is being carried out.

Due to a change in data protection legislation, confidential references are no longer available to individuals as part of their Right to Access. Although the University is not required to release this information to applicants upon request, in the interests of good practice and transparency, we will continue to adhere to this practice unless you specifically detail on the reference that it is confidential and should not be disclosed.

You have some obligations under your employment contract to provide the University with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the University with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the University to enter a contract of employment with you. Data cannot be withheld from the Home Office on their request if you are a sponsored employee (sponsored under the points based immigration system) and in receipt of a Tier 2, Tier 4 or Tier 5 visa. If you do not provide other information, this will hinder our ability to efficiently administer the rights and obligations arising from and associated with the employment relationship.

Complaints

If you wish to raise a complaint on how we have handled your personal data, you can contact the University Data Protection Officer who will investigate the matter.

Our Data Protection Officer can be contacted at dataprotectionofficer@glasgow.ac.uk

If you are not satisfied with our response or believe we are not processing your personal data in accordance with the law, you can complain to the Information Commissioner's Office (ICO) https://ico.org.uk/