



## Privacy Notice: Staff and Other Individuals who Work with the University in a Paid or Unpaid Capacity

Privacy Notice
<p>This privacy notice explains how the University of Strathclyde will use your personal information and your rights under data protection legislation. This notice relates to individuals in the categories of: employee; worker; assignee; volunteer; trainer; external secondee; visiting/honorary member of staff; consultant; agent; contractor; and collaborator. A separate privacy notice is available for Court members/trustees.</p>
Who we are
<p>The University of Strathclyde is the organisation responsible for your personal data and making sure it is processed in line with data protection legislation (the data controller).</p>
Information we collect and use about you
<p>We obtain personal data about you from a variety of sources including (but not limited to):</p> <ul style="list-style-type: none"> <li>• directly from you in your application (including references from individuals you have listed);</li> <li>• during your employment/engagement with the University, e.g. Annual Development Reviews and updates you make to your personal details stored on University systems, e.g. Pegasus</li> <li>• as a result of any University policies/procedures e.g., disciplinary/complaints; and</li> <li>• from agencies from which we are legally obliged to seek information (such as Disclosure Scotland and previous employers).</li> </ul> <p>Personal information may be held in electronic or hard copy format relating to:</p> <ul style="list-style-type: none"> <li>• personal and contact information (including emergency contacts);</li> <li>• education records (including qualifications, skills and personal statements);</li> <li>• evidence of your right to work in the UK;</li> <li>• provision of, access to and use of IT systems and information;</li> <li>• employment and training details;</li> <li>• references;</li> <li>• banking details;</li> <li>• casework and attendance records;</li> <li>• goods or services provided;</li> <li>• visual images; audiovisual recordings</li> <li>• occupational health, safety and wellbeing.</li> </ul> <p>‘Special category data’ relates to: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data or biometric data (where used for identification purposes); health; sex life; and sexual orientation.</p> <p>This data is subject to additional protections. In most cases for special category data you have the option whether or not to provide this information (or the option to choose ‘prefer not to say’).</p> <p>Data relating to criminal convictions and offences is also subject to strict processing requirements and is only processed when necessary and in accordance with the law. This data will be held for the minimum amount of time necessary.</p> <p>For certain roles, you will need to apply to <a href="#">Disclosure Scotland</a>, this includes posts requiring clearance under the Protection of Vulnerable Groups (PVG) scheme. The University will countersign your form and will be notified of the outcome; in such cases, obtaining relevant clearance may be a condition of your continuing employment with the University. All Academic and Learning and Teaching roles will</p>

require a basic disclosure as a condition of employment with the University. Relevant information will only be retained for as long as necessary for recruitment and administrative purposes. Some roles may also require enhanced security vetting, you will be advised if this relates to your role.

### **Why we require this information and our lawful basis**

The University collects, holds and uses a wide range of information about you for various reasons including:

- managing your contract of employment with the University;
- providing IT and other essential services;
- disciplinary, grievance and complaints processes;
- administrative and financial management purposes;
- academic, learning and teaching, and research purposes;
- performance management;
- to meet our duty of care to you;
- to meet our legal obligations;
- public safety and the prevention and detection of crime;
- archiving and research purposes;
- promotion of the University;
- issuing and managing internal communications, surveys etc.
- ensuring health and safety (including monitoring);
- ensuring equality of opportunity;
- providing occupational health services;
- attendance/absence management (includes leave of any kind and medical information submitted, where appropriate);
- management and security of the campus/estate and facilities (including CCTV and access management);
- equal opportunities monitoring;
- responding to and defend against legal claims;
- dealing with emergency situations (at an individual and University level). This includes maintaining lists of emergency contacts both personal and business.

The University requires a lawful basis for processing personal data. In some cases, there may be more than one lawful basis that applies. Most routine processing of staff data is on the lawful basis of public task and/or contract (managing your contract of employment). However, we may rely on any of the following lawful bases, depending on the circumstances:

- consent;
- contract;
- legal obligation;
- vital interests;
- public task;
- legitimate interests.

Special category data can be processed when one of the lawful bases listed above applies **and** an additional lawful basis. Most processing of special category data is done on the basis of explicit consent and/or substantial public interest e.g. in relation to equality of opportunity. However, we may rely on any of the following lawful bases, depending on the circumstances:

- explicit consent;
- vital interests;
- establishment, exercise or defence of legal claims;
- substantial public interest;
- preventive or occupational medicine;
- public interest in the area of public health;
- archiving in the public interest, scientific or historical research purposes or statistical purposes.

### **Disclosing your information**

In some situations the University will share your personal data with external organisations. Often this is where we have a contractual agreement with an organisation to provide services to us, or we have a legal obligation to provide information e.g.:

- payroll and pension administrators/providers;
- insurers and auditors;
- organisations involved in funding, accrediting or reviewing the quality of
- bodies who administer background and/or criminal records checks, e.g. Disclosure Scotland;

University activities, including research, e.g. Scottish Funding Council, Higher Education Funding Council for England (including for the Research Excellence Framework);

- to obtain pre-employment references
- partner organisations involved in joint/collaborative course provision or where staff participate in teaching/administrative staff mobility or exchanges;
- relevant government agencies, e.g. HMRC, Home Office, UK Visas and Immigration;
- Higher Education Statistics Agency (HESA - [now part of Jisc](#)). See also [HESA Staff Collection Notice](#);
- law enforcement agencies;
- relevant authorities dealing with emergency situations at the University;
- travel management providers;
- potential employers;

- professional, statutory and regulatory bodies e.g. Scottish Public Services Ombudsman, Office of Scottish Information Commissioner; Information Commissioner's Office; Health & Safety Executive;
- Accreditation bodies, e.g. Advance HE, BALEAP;
- Collective organisations of which the University is a member, such as the Universities and Colleges Employers' Association (UCEA), and other agencies with which the sector collaborates for employer benchmarking purposes;
- affiliated external providers of facilities/services you have chosen to utilise/receive, e.g. third party parking providers;
- providers of occupational health and other services/support;
- for staff employed and paid outside the UK: relevant bodies/agencies in that territory/country to meet legal obligations
- any other authorised third party to whom the University has a legal/contractual obligation to share data with.

The University makes some information publicly available via its website to enable individuals, including students, potential students and research partners to identify individuals they wish to communicate with. Your name, department/section, job title, email address and telephone number will normally appear in the University's staff and telephone directory. Staff may choose to provide an image of themselves to accompany their entry in the staff directory. If you submit a personal statement and a photograph within any self-service HR system/process, these will become publicly-available via the Staff Search pages of the University website.

It is expected that staff, particularly those involved in learning, teaching and research, will provide information to be published on the website for academic/business purposes including academic qualifications and professional recognition, brief biography, professional/research interests, activities and outputs. Research outputs are held in the University's research repository, PURE, and will identify academic/research staff involved.

Certain activities, such as lectures, may be recorded or audio recorded to support online learning, or to implement recommended reasonable adjustments for staff or students with disabilities or additional requirements.

Appropriate information and/or signage will be provided prior to any media/photography taking place, including for publicity purposes. If it is necessary, consent will be obtained.

### **Transferring data internationally**

Some personal data may be transferred outside the UK for example:

- where the University is involved in collaborations/course provision with or for organisations and educational institutions overseas,
- where the University is involved in staff and student exchanges and academic partnerships;
- where the University works with overseas student recruitment agencies and partner institutions limited staff data may be transferred;
- information published on the University's website is accessible internationally;
- the University may engage third parties to provide systems/services which are hosted outside the UK;

- in emergency situations for international staff we may transfer data internationally where it is necessary to ensure your vital interests, e.g. contacting next of kin in medical emergencies.

Whenever we transfer data internationally we will make sure that appropriate safeguards are in place to protect your information and your rights to privacy.

#### **Keeping your information up to date**

The University strives to ensure that your personal data is accurate and up-to-date. Staff also have a responsibility to update changes to their contact information via the relevant HR system. In addition, you should advise the University of any inaccuracies in the personal data held about you.

#### **How long your information is retained**

Retention periods for staff records held and managed by Human Resources are as set out in the University's HR retention schedule. Staff data held in other areas may be subject to different retention periods. University retention schedules can be accessed online via our website <https://www.strath.ac.uk/ps/strategyandpolicy/recordsmanagement/>.

Please note, after you cease to work with the University, we will still require to hold your personal data for a period of time to satisfy statutory/legal obligations and/or to meet administrative requirements. Limited, anonymised data will also be retained to allow the University to perform statistical analyses.

#### **Data required as part of a statutory or contractual requirement or obligation**

Some information must be processed by the University in order to manage your contract or because we have a legal obligation. For example, contact details, your right to work in the UK and payment details. The University is also legally required to supply information to the Home Office on request, e.g. in relation to staff who are working under certain types of visa.

If you do not provide, as a minimum, the information required by the University to meet its legal obligations, it will not be possible to employ or work with you. In any case, withholding necessary information will hinder your ability to work and the university's ability to administer your contract and the rights and obligations arising as a result of the employment relationship.

#### **Your rights**

Under data protection legislation, you have a number of rights\* including the right to:

- withdraw consent, at any time, where that is the lawful basis of our processing;
- access your personal data and obtain a copy, free of charge;
- rectify inaccuracies in personal data that we hold about you;
- erasure, i.e. have your details removed from systems we use to process your personal data;
- restrict the processing in certain ways;
- obtain a portable copy of data you have given to us in a commonly used electronic form; and
- object to certain processing of your personal data by us.

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

Please contact [dataprotection@strath.ac.uk](mailto:dataprotection@strath.ac.uk) if you wish to exercise/enquire about any of these rights.

#### **Complaints**

If you wish to make a complaint about how we have handled your personal data, you can contact the Data Protection Officer at [dataprotection@strath.ac.uk](mailto:dataprotection@strath.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 also have the right to complain to the Information Commissioner's Office (<https://ico.org.uk/concerns/>).