

Privacy notice for employees, workers and contractors

WHAT IS THE PURPOSE OF THIS DOCUMENT?

UHI North, West and Hebrides is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with data protection legislation, including the General Data Protection Regulation (GDPR) and Data Protection Act 2018, and may be amended from time to time.

UHI North, West and Hebrides is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services.

It is important that you read this notice, together with any other privacy policies or privacy notices we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses;
 - Date of birth;
 - Gender;
 - Information about your marital status, next of kin, dependants and emergency contacts;
 - National Insurance number, bank account details, payroll records and tax status information;
 - Salary, annual leave, pension and benefits information;
 - Start date;
 - Location of employment or workplace;
 - Terms and conditions of your employment;
-

- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process);
- Employment records (including job titles, work history, working hours, training records and professional memberships);
- Compensation history;
- Assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- Details of any disciplinary or grievance procedures in which you have been involved including any warnings issued to you and related correspondence;
- Details of your days of work, working hours and attendance at work;
- Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- Photographs.

For some senior posts we will collect, store, and use the following additional categories of personal information about you:

- Details of other appointments, offices and Directorships, including any formal positions/connections with other educational institutions.
- Details of any kinship relationships within the College or University
- Details of significant shareholdings and involvement in contracts.

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

- Information about your race or ethnicity, religious beliefs and sexual orientation.
- Information about your health, including any medical condition and whether or not you have a disability for which the College needs to make reasonable adjustments, health and sickness records.
- Information about criminal convictions and offences.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments. We

may sometimes collect additional information from third parties including former employers or other background check agencies, e.g. Disclosure Scotland.

Data is stored in a range of different places, including in your personnel file, in the College's HR management systems and in other IT systems (including the College's email system and JISC UHI Online surveys).

HOW WE WILL USE INFORMATION ABOUT YOU

The College needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs 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.

In some cases, the College needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws, to enable employees to take periods of leave to which they are entitled, and to consult with employee representatives if redundancies are proposed or a business transfer is to take place. It is also necessary to carry out criminal record checks to ensure that individuals are permitted to undertake the role in question.

We may also use your personal information in the following situations, which are likely to be rare: 1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes (e.g. Scottish Funding Council).

Situations in which we will use your personal information

We need all the categories of information listed primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment;
- Determining the terms on which you work for us;
- Checking you are legally entitled to work in the UK;
- Paying you and, if you are an employee, deducting tax and National Insurance contributions;
- Liaising with your pension provider;
- Administering the contract we have entered into with you;
- Business management and planning, including accounting and auditing;
- Conducting performance reviews, managing performance and determining performance requirements to plan for career development, and for succession planning and workforce management purposes;
- Making decisions about salary reviews and compensation;

- Assessing qualifications for a particular job or task, including decisions about promotions;
- Gathering evidence and recording disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- Making decisions about your continued employment;
- Making arrangements for the termination of our working relationship;
- Education, training and development requirements;
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- 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;
- Obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- Complying with health and safety obligations;
- To prevent fraud;
- To understand and prevent any Conflict of Interests which may arise
- To monitor your use of our information and communication systems to ensure compliance with our IT policies;
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates;
- Equal opportunities monitoring;
- To 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;
- 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 College 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;
- Ensure effective general HR and business administration;
- Conduct employee engagement surveys;
- Provide references on request for current or former employees;
- Maintain and promote equality in the workplace;

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 and for health and safety purposes).

Where the College processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the College uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

If you fail to provide personal information

You have some obligations under your employment contract to provide the College 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 College 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 College to enter a contract of employment with you. If you do not provide other information, this will hinder the College's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Who has access to data?

Your information will be shared internally, including the HR department, payroll, your line manager, managers in the area in which you work and IT staff if access to the data is necessary for performance of their roles.

Your data may also be shared with employee representatives in the context of collective consultation on a redundancy or business sale.

The College shares 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 from Disclosure Scotland. The College may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The College also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services.

The College will not transfer your data to countries outside the European Economic Area.

How secure is my information with third-party service providers.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

“Special categories” of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our Data Protection Policy.
3. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
4. Where you have already made the information public.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leave, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our Data Protection Policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Data Protection Policy.

We require to obtain and retain a satisfactory PVG check prior to and for the duration of your employment.

DATA RETENTION

How long will you use/hold my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Records Management & Archiving Policy which is available from the staff area.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our Data Protection Policy and applicable laws and regulations.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you.
- **Request correction** - This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** - This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** - Where we are relying on a legitimate interest (or those of a third party) and there is something which makes you want to object to processing on this ground.
- **Request the restriction of processing** - This allows you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party when the information is stored and processed automatically.

If you want to exercise any of the above rights, please contact the Data Protection Officer dataprotectionofficer@uhi.ac.uk in writing.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer dataprotectionofficer@uhi.ac.uk.

DATA PROTECTION OFFICER

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Officer dataprotectionofficer@uhi.ac.uk.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO) www.ico.org.uk, the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the Human Resources department nwh.hr@uhi.ac.uk