For Employees
Feb 2021

MORAY COLLEGE UHI PRIVACY NOTICE

PRIVACY OF INFORMATION

The College 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 law.

This document applies to all employees, workers and contractors. The College 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.

It is important that you read this notice, so that you are aware of how and why we are using your personal information and of your rights in relation to your data.

ABOUT MORAY COLLEGE UHI

Moray College UHI and the University of the Highlands and Islands (UHI), The University of the Highlands and Islands Development Trust and Academic Partners are registered with the Information Commissioner's Office (ICO) as required by the Data Protection Act. The personal data that you supply is held and processed by Moray College and UHI and/or the academic partner(s) which constitute the University of the Highlands and Islands (UHI), as laid out in the requirements of the Further and Higher Education (Scotland) Act 1992.

Moray College UHI is registered with the ICO, registration number Z4664882.

HOW WE LOOK AFTER YOUR PERSONAL DATA

The General Data Protection Regulation (GDPR) is a significant update to the data protection act. The act requires us to tell you how we comply with data protection law. This act says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The College has in place a policy and procedure framework to ensure data is kept secure and processed in line with the data protection act. Please see R:\GDPR for full details of relevant policies.

PERSONAL DATA HELD ABOUT YOU

Personal data, or personal information, means any information which identifies you. It does not include data where the identity has been anonymised or aggregated.

There are "special categories" or more sensitive personal data which require a higher level of protection.

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.
- Marital status and dependants.
- Next of kin and emergency contact information.
- 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.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in an application form, CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, time off, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- Information about your use of our information and communications systems.
- Photographs.

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

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade Union membership.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

SMS Text Messaging

If you have provided consent to share the mobile number you have configured within HR World Service to be used within the College's SMS text messaging platform, this number will be used to send emergency information. This is limited to College emergencies covering site safety issue, severe weather warnings and College closure information. Only the mobile number will be used for this process and the message sent may be retained in the SMS platform for a maximum of 6 months.

HOW YOUR PERSONAL INFORMATION IS COLLECTED

Personal data is collect during the application and recruitment process, either directly from candidates or sometimes from 3rd parties such as employment agencies. We may sometimes collect additional information from former employers and Disclosure Scotland.

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

DATA PROCESSING

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

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.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. 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 that you are legally entitled to work in the UK
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing staff benefits to you.
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting staff reviews.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination or our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our Information Security Policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communication systems and preventing malicious software distribution.
- To conduct monitoring of data to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- Advising you of vacancies or opportunities for work

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

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.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, only where this is required or permitted by law.

WHAT HAPPENS IF YOU DO NOT PROVIDE PERSONAL INFORMATION TO THE COLLEGE

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our staff and students).

It is also 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.

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 the College data Protection policy.
3. Where it is needed in the public interest, such as for equal opportunities and in line with our data protection policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

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

Our obligations to you as an employer in relation to your sensitive personal information

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

- We will use information relating to leave of absence, which may include sickness absence or family related leaves, 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, where you have shared it with us, about your age, caring responsibilities, disability status, gender identity, marital or civil partnership status, pregnancy or maternity/paternity status, nationality and ethnic origin, religious, philosophical or moral beliefs, sex, or sexual orientation. Doing so ensures meaningful equality monitoring and reporting, in support of our legal duties and in the public interest. Although when gathering this particularly sensitive personal information we provide a

'prefer not to say' option, more information allows us to make positive improvements, so we encourage you to provide this confidential information if you feel able to do so.

- We will use trade union membership information to pay trade union premiums and to comply with employment law obligations.

Do we need your consent to use this data?

We do not need your consent if we use special categories of your personal information in accordance with policy and 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. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

WHEN WE MAY USE 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.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or some else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about relevant criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about relevant criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of your working for us or by Disclosure Scotland. We will use information about criminal convictions and offences in the following ways.

AUTOMATED DECISION-MAKING

We do not envisage that any decisions will be taken about you using automated means, however we will notify you if this position changes.

DATA SHARING – WHY WE MAY NEED TO SHARE YOUR DATA

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law.

Our Data Protection Policy places extra restriction on the transfer of your personal information outside the EEA. In circumstances where this takes place, adequate protection to the same level as the General Data Protection Regulation is required.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate and lawful interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents). The following activities are carried out by third-party service providers: pension administration and occupational health services.

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

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our contractual terms and conditions. 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.

What about other third parties?

We may need to share your personal information with regulatory bodies, Scottish Government, Scottish Funding Council, or related entities to otherwise comply with the law. The information we share will be proportionate, relevant and not excessive and where possible it will be anonymised.

DATA SHARING – THE NATIONAL FRAUD INITIATIVE

This section describes how College collects and processes your data under our legal obligations regarding the National Fraud Initiative (NFI). Data sharing is covered by law.

The NFI is a data matching exercise which matches electronic data within and between participating bodies to prevent and detect fraud.

The College is required to comply with NFI Security Policy and all College staff are in scope. This requires us to share payroll with the following agencies:

- Audit Scotland which carries out data matching under part 2A of the Public Finance and Accountability (Scotland) Act 2000 which is the lawful basis used by the College to share the information.
- The Cabinet Office which processes the data for NFI in Scotland on behalf of Audit Scotland, and provides its secure website and NFI application for participating bodies and auditors in Scotland to use.

Other relevant parties to the data sharing are:

- The Auditor General for Scotland.
- Accounts Commission for Scotland.

Information is shared securely for the prevention and detection of fraud or another permitted purpose in line with the act described above.

DATA SECURITY

The UHI Partnership Information Security Policies have been formally adopted by Moray College. This framework, together with a range of network and physical security measures have been implemented to protect the security of your information. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

All staff are required to keep up to date with Information Security training to help raise awareness and promote good practice.

The measures we have put in place will are designed 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 employees, agents, contractors and other third parties 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 and must comply with the law.

The College Data Breach Handling Policy and Procedure will deal with any suspected data security breach. In any such circumstances, we will notify you and the Data Protection Officer of any suspected breach. Our policy requires the College to consider if any breach meets the test for reporting to the ICO, as required by law.

RETENTION OF PERSONAL DATA

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 Retention Policy To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

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 Records Retention Policy and applicable laws and regulations.

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. If you do not keep us informed of changes we may be prevented from performing the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure your health and safety and the health and safety of our staff and students).

YOUR RIGHTS OF ACCESS, CORRECTION, ERASURE AND RESTRICTION

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

- Request access to your personal information (commonly known as “data subject access request”).
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask 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 of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- Request the restriction of processing of your personal information. This enables 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.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the College’s Data Protection Officer in writing (see below for details).

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

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 College's Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

THE COLLEGE DATA PROTECTION OFFICER

The UHI Partnership has 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 DPO by email at dataprotectionofficer@uhi.ac.uk.

For any other general enquiries, then please contact Human Resources.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. This is outlined in our Data Protection Policy.

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.

This notice applies to current, prospective and former employees and contractors. This notice does not form part of any contract of employment.