UHI Moray

Data Protection Policy

Status	Approved
Version Date and Number	15/3/23 V1.1
Approved by	F&GP Committee
Responsibility for Policy	Director of Information, Planning and Student Support
Responsibility for Implementation	All College Employees
Responsibility for Review	Director of Information, Planning and Student Support
Date for Review	03/26

Please ask if you, or someone you know, would like this document in a different format or language.

Revision Date & Change Log

Date of Revision	Brief Description of Change	Date Approved
25/05/18	V0.1 First issue on GDPR Launch Day	25/5/18
06/06/18	V0.2 Minor corrections	6/6/18
02/11/18	V1.0 Updated guidance on email use for staff and adoption of UHI Legitimate Interest Assessment	5/3/19
10/02/23	V1.1 New UHI Moray branding, replace GDPR with DPA, minor revisions to text.	15/3/23

Table of Contents

1. Introduction

UHI Moray is a data controller and processor of personal data held in relation to staff, students and other 3rd parties in connection with all business related to the College.

The College is registered with the Information Commissioner's Office (ICO) as a public authority with registration number **Z4664882** in accordance with the requirements set out in the UK Data Protection Act (2018) (DPA) and General Data Protection Regulation (GDPR).

The College's registration with the ICO also covers the College as a Scottish Public Authority under the Freedom of Information (Scotland) Act 2002.

This policy provides a clear statement on how UHI Moray controls all aspects of data protection from data capture, security, storage, processing, sharing and disposal in line with the DPA and GDPR.

The policy also provides a clear guide for all staff on how to comply with data protection principles and respond to data protection related issues.

2. Scope

This policy applies to all staff employed by UHI Moray who have a duty to ensure that all data covering staff, students, suppliers, visitors and partners is kept secure and processed lawfully.

All personal data stored both within the College, the UHI partnership (i.e. The University of the Highlands and Islands and the Academic Partners) and official 3rd party cloud providers contracted by the College and UHI are fully in scope of this policy.

3. Responsibilities

The College's nominated independent Data Protection Officer (DPO) is responsible for:

- Supporting data breaches and liaison with the ICO.
- Monitoring the College's compliance with data protection legislation.
- Providing advice to the College executive and Board of Management.

The Director of Information, Planning and Student Support (IPSS) is responsible for:

- Review and update of this policy and procedure.
- Monitoring and reporting compliance issues to the DPO.
- Promotion of good practice, policies and procedures.
- Registration of the College with the ICO.

The Director of HR and Organisational Change is responsible for:

- Maintaining records of staff data protection training.
- Maintaining the College's on-line training portal with DPA related courses.

Line Managers are responsible for:

- Ensuring records are processed in line with departmental records management policies.
- Ensuring data protection practice is effective within their department.

All staff members are responsible for:

- Following this policy and ensuring that information is stored and processed lawfully.
- Undertaking mandatory UHI Information Security Training at induction and biannual refresher training.
- Reporting data protection issues or breaches.

4. Data Protection Officer (DPO)

The College designated DPO is employed by the University and Colleges Shared Service (UCSS) on behalf of the UHI Partnership. The responsibilities of the DPO are highlighted in section 3 above.

The Director of IPSS is the Strategic Leadership Team (SLT) member with executive level responsibility for data protection in College.

5. Data Protection Compliance

The following compliance areas cover how the College maintains information security:

- **Awareness** – All staff are required to undertake training at induction and regular refresher training to keep up to date with good practice in data security.
- **Records Management** – The College has in place a Data Asset Register which records all record types used in College. Departmental level Records Management Policies for staff provide clear guidance on record processing, retention and disposal.
- **Communicating Privacy Information** – Privacy notices outline to data subjects how data is processed and complies with the DPA. The Personal Electronic Communication Regulation (PECR) is also covered by policy to regulate direct marketing activities.
- **Individuals Rights** – Policies and procedures reflect individuals rights under GDPR:
    - The right to be informed about the use of personal data.
    - The right to access via subject access requests.
    - The right to rectification - we must respond to requests to correct errors.
    - The right to erasure, in compliance with statutory retention requirements.

  - The right to restrict processing of data.
  - The right to data portability e.g. to support a student transferring elsewhere, to make it easier to take their data with them.
  - The right to object to processing.
  - The right not be subject to automatic decision making, including profiling.
  - These rights are covered by policy and are outlined in privacy notices – please see the Privacy and Marketing Communication Policy for details.

- **Right to Access (Subject Access Request – SAR) –** a policy and associated procedures for SAR processing is in place to enable data subjects to find out what the data the College holds about them.
- **Lawful Basis for Data Processing** – The College Data Asset Register has established the legal basis for processing all record types in College.
- **Consent** – Policies and procedures are in place for data subject consent for data processing. This is particularly important in terms of marketing data and communication methods (PECR) and is covered by policy.
- **Children** – Safeguards are in place to ensure processing of children's data has appropriate parental or guardian consent. Services must be designed with children in mind and processing activities restricted in terms of children's data.
- **Data Breaches** – The College has a data breach procedure to manage data breaches and, where required covers ICO reporting requirements.
- **Data protection by Design –** Requests for new software or new projects must fully consider data protection as a key project requirement at the earliest stage possible.
- **Privacy Impact Assessments –** The College has adopted the UHI Privacy Impact Assessment tool.
- **Data Protection Officer** – The College has appointed a DPO who acts independently of the College executive as described in section 4 above.
- **International** – This policy requires staff to seek specific advice prior to engaging in any cross-border trade in personal data, both within and outside the EEA.

6. Data Sharing

Data must not be shared with any 3rd party unless there is statutory requirement to do so or, a formal data sharing agreement and/or contract is in place.

Privacy Notices must inform all data subjects where data sharing takes place with 3rd parties and must indicate the established legal basis for sharing, including where any consent has been obtained.

Sharing of personal data outside the boundaries highlighted in a privacy notice will require additional consent to avoid the potential for a data breach, unless the sharing is covered by a legal basis.

6.1 3rd Party Data Processors

The College is responsible for ensuring that any data processed by 3rd party data processors is compliant with the DPA.

A Privacy Impact Assessment (PIA) must be carried out during the negotiation of any new contract with a 3rd party data processor to ensure all relevant safeguards are in place. Such documentation must remain in place for the entire duration of any such contract.

7. Requests for Information

Staff regularly deal with requests for information from a data subjects. In all cases, the identity of the data subject must be verified prior to any release of information.

Enrolled students must present a photographic identification, preferably a student ID card and, in cases where contact is by email or telephone, staff must ensure that email addresses and phone numbers are consistent with data officially recorded in College systems.

If verification is not immediately possible, the data subject may be asked to present in person with identification.

Staff requests for personal related data should be directed to Human Resources.

All other requests should be directed to the Principal’s office who will route the request to the appropriate section.

More detailed or complex requests for information are likely to fall under the **Subject Access Request (SAR) Policy and Procedure.** SARs should use the on-line SAR submission form, but any other written forms of submission are acceptable.

Requests for information about data subjects from Police Scotland are handled differently and covered in **Section 8** below.

7.1 Consent

Students aged 16 and over must provide relevant consent for handover of information to 3rd parties where the sharing is not covered by statutory act or is outside of Privacy Notices signposted at enrolment. Parents or carers must provide consent for those aged under-16.

Non-routine sharing of staff data outside of the established Staff Privacy Notice is likely to require consent unless covered by an established legal basis.

Schools Link Pupils

All requests for information related to pupils enrolled on College-School links programmes must be referred to the Local Authority. The Head of Academic Partnerships or member of the Strategic Leadership team must be made aware of any such requests.

Requests from 3rd Parties about a Data Subject (not SAR)

Requests about data subjects from 3rd parties must consider the legal basis for sharing personal data and whether or not consent is required. All requests must be logged with the Director of IPSS.

A range of government agencies have special access to data without the consent of a data subject. Staff must take care to ensure that these requests are routed to an appropriate senior manager. This is likely to cover situations involving:

- Court proceedings.
- Legal Orders e.g. debt collection.
- Collection of taxes and benefits (which are routinely managed within the Administration Services Centre and Human Resources Section).

Routine requests from any other external agency, company or private individual must have appropriate consent from the data subject in place prior to the release of any information.

The identity of the 3rd party must be verified in all requests.

8. Personal Data Requests from Police Scotland

8.1 General Guidance

In the event of an emergency, information should be passed to Police Scotland without delay.

In almost all circumstances, the release of personal data to Police Scotland is in relation to an on-going official Police enquiry and is likely to cover:

- CCTV footage.
- A limited range of College employee data.
- A limited range of Further Education Student data, but in the case of schools link pupils, the relevant school must be contacted immediately before any release of data.

Where practical, requests should be in writing.

Requests for Higher Education student data should be referred to the UHI Student Records Office.

8.2 Request to Interview a Student (FE and HE)

Police Scotland officers regularly need to engage with students on-campus and the procedure is as follows:

- Reception staff should refer the Police Officer to the Administration Services Centre Manager (or Principal's office if unavailable).
- The manager must check that the request is in line with an on-going Police enquiry, in line with the DPA.
- If a schools-link pupil is involved, the relevant school should be contacted first and the Police should be referred to the School.
- Care must be taken to identify the student and arrangements made for private space to be used for any meeting.

These situations will normally require the release of student contact details and timetable data.

In the event that the student is not in College, then FE details should be released and, unless there is an emergency situation, release of HE data should be approved by the UHI Student Records Office.

8.3 Special Exemptions

Regardless of which organisation is data controller, personal data must be released immediately for the protection of life.

In these circumstances, staff can release information immediately to avoid any delay during any emergency. The University (as HE student data controller) must always be informed of any such data release, including the nature of the release and the student details.

9. Data Storage and File Encryption

The UHI Partnership Information Security Policies have been adopted and all College laptops and external storage drives enforce the use of Microsoft BitLocker drive encryption.

Staff may only store personal data on approved College data stores.

Personal data stores such as 3rd party hosted file systems, USB drives or other mobile devices must never be used to store personal data about a data subject, unless specifically authorised by the College or UHI, in line with the Partnership Information Security Policies.

All external drives used by staff must be encrypted and this is enforced by network security policy.

10. Data Sharing Outside the EEA

The College shares data with companies and partners located within the EEA. Any activity likely to require sharing of data outside of the EEA requires notification to the Director if IPSS in the first instance and completion of a PIA.

Where suppliers have been fully assessed, consideration for storing personal data outside the EEA will only be approved where:

- There is no alternative option within the EEA e.g. no available specialist supplier of goods or services and the service is critical to the College.
- Data Protection standards of the country meet the standards set out in GDPR.
- The transfer has been reviewed and approved by the DPO.

Staff must take particular care when using Internet hosted services as these can lead to data being stored outside the EEA, even though the service has been procured inside the EEA.

A privacy impact assessment must be carried out when storing any data off-campus.

11. Data Breaches

The College has in place a **Data Breach Policy and Procedure**. All breaches must be reported and managed under the policy.

Breaches must be reported to the Director of IPSS, or if not available, immediately to the Duty Head. In all cases, the DPO must also be informed.

The policy outlines key statutory reporting deadlines which must be adhered to.

12. Processing Sensitive Personal Data

Staff must ensure extra safeguards are in place when handling sensitive personal data. The College routinely captures sensitive data for a range of functions:

- Staff recruitment processes and general management of staff.
- Board member recruitment.
- Student application and enrolment.
- Student academic and support processes.

The processing of sensitive personal data covers:

- Marital Status.
- Ethnicity.
- Religion.
- Trade-union subscriptions (staff only).
- Healthcare related data (including any medical condition of a data subject).
- Sexual orientation.
- Care Experience.
- Current Gender Identity.
- Photo ID.

- Personal opinion.
- Location Data, including IP Addresses.

12.1 Sharing and Storage of Sensitive Personal Data

Data in this category must be reported internally at aggregated level or be anonymised to protect the identity of data subjects. Data sharing agreements must be specific with full consent in place prior to any external sharing of such data, unless covered by a statutory requirement.

Access to raw personal data is restricted in College and must never be stored on the open areas within SharePoint or other file stores.

Email must never be used to send raw sensitive personal data outside the organisation, unless it is fully encrypted using 256 bit encryption. ITU staff can provide guidance on using the secure email service.

The Scottish Funding Council (SFC) and other agencies provide secure web portals for sharing data.

Staff wishing to use any raw data covering these categories should seek advice from the Director of IPSS first and carry out a PIA for any new proposed activities.

12.2 Photographs

Photographic ID of staff and students are stored electronically in SITS for security purposes.

Staff are permitted to take photographs of College activities as long as the context is established e.g. photographs of a specific event, celebration or classroom activity where everyone in the photo has provided verbal consent to being photographed.

Staff must also note the need for specific parental or guardian consent for those aged under 16 and seek guidance from the local authority for any event involving school pupils.

Taking individual photographs of students for a specific purpose outside of regular activity will require a full privacy notice to be issued and consent formally obtained.

If compliance is unclear, then staff should confirm arrangements with the Director of IPSS prior any planned activity.

Photographs must be considered as personal data and the full rights of all individuals is signposted in the marketing Privacy Notice is published at:

http://www.moray.uhi.ac.uk/t4-media/one-web/moray/about-us/publications/corporate/Marketing-Privacy-Notice.pdf

13. Use of Email and Personal Data

13.1 Acceptable Use and Risk

The ICT Acceptable Use Policy for staff outlines general guidance for the use of ICT, with the use of Email being a high risk area due to:

- The high volume of emails delivered each day.
- The high volume of registered staff and student email accounts.

Staff must take extra care to ensure personal data in emails is limited and appropriate for the purpose it's being used.

13.2 General Principles

When sending email, staff must:

- Consider whether email is the most appropriate way to convey personal data.
- Take appropriate steps to ensure that emails are addressed only to the intended recipients i.e. internal staff emails use the format *forename.surname***.moray@uhi.ac.uk**.
- Use College email accounts only to conduct business related to the College, however it's recognised that employees may need to share their email address with other agencies and companies e.g. employee approved discount schemes or registration with professional bodies. Staff must ensure that any 3rd party site registered with a College email account implements a unique password.

There are multiple email accounts with very similar email addresses, including student accounts, therefore the risk of a data breach is high.

13.3 Use of Personal Data in Email

Staff must limit personal data and restrict expressing personal opinion in an email to a wider audience within the UHI partnership. Forwarding emails without considering the content also poses a risk of data breach.

Personal data must never leave the UHI network unless encryption has been implemented and there are controls in place to manage data transfers. The UHI secure drop box service provides a secure method to send data safely.

Student data must never leave the College network unless authorised by the MIS Analyst.

Staff data is the responsibility of the Human Resources Section and routine data sharing is limited to authorised staff.

Staff should also note that emails are in scope for:

- Freedom of Information Requests (in some circumstances).
- Subject Access Requests

13.4 Good Practice

Email accounts should not be used as a permanent repository to store data files. Staff should be aware of the College's records retention policies and ensure that redundant emails are securely deleted.

Email subject lines should not contain personal data since there is a risk they could be read by others.

An email address is personal data and when sending out emails to multiple external organisations or contacts, using the Blind Copy (or bcc function) is essential to ensure email addresses are kept secure.

14. Privacy Notices

Privacy notices must make it clear to data subjects what their rights are, how their data is being processed and how the College approaches information security and data sharing. They are issued to:

- Students at application and enrolment.
- Staff at commencement of employment (and when updated, to all current staff).
- Visitors to http://www.moray.uhi.ac.uk (link is provided on the footer of the front page).
- Direct marketing contacts.
- To others as and when required e.g. survey activity.

Where the basis for processing data is based on Legitimate Interest, then the UHI Legitimate Interest Assessment form must be completed. This is available on the College Intranet and advice is available from the Director of IPSS.

The privacy notice master template can be found in the **Privacy and Marketing Communication Policy** which adopts the UHI Privacy Notice toolkit.

All public facing websites must incorporate the standard web privacy notice available from the Director of IPSS.

15. College Data Protection Contacts

Routine requests for advice or to raise any concerns about data protection in UHI Moray should be sent to dataprotectionofficer@uhi.ac.uk or by writing to:

The Data Protection Officer
UHI Moray
Moray Street
Elgin
Moray
IV30 1JJ

Formal complaints about data protection will be dealt with by the DPO in line with the College Complaints Procedure.

16. Complaining to the ICO

The College data breach policy provides clear guidance on reporting to the ICO. Any individual who has concerns about the College's processing of data under the terms of the DPA may complain to the ICO at:

- ICO Website: https://ico.org.uk/concerns/
- ICO telephone helpline: 0303 123 1113

All liaison with the College must involve the DPO.

17. Relevant College Policies and Procedures

Data Breach Policy and Procedure
College Privacy Notices
Privacy and Marketing Communication Policy
Subject Access Request Policy and Procedure
Right to Erasure Policy and Procedure
UHI Partnership Information Security Policy Framework
Student Confidentiality Policy
IT Acceptable Use Policy for Staff
IT Acceptable Use Policy for Students