UHI | INVERNESS

DATA PROTECTION POLICY

PL/GO/2023/001

Lead Officer	College Principal & Chief Executive
Review Officer	Information Development Manager
Date first approved by BoM	27 November 2009
First Review Date	25 May 2010
Date review approved by BoM	August 2023
Next Review Date	June 2026
Equality impact assessment	Yes

Reviewer	Date	Amendments
Information Development Manager	16/08/	Update to legislative/policy & procedure references and included additional responsibility to the Principal & Chief Exec. Some language amendments made but the context remains the same.

1. Policy Statement

UHI Inverness is committed to ensuring that the processing of personal data is only undertaken in the legitimate operation of the college's business.

The college collects and uses information (data) about its staff, students and other individuals and bodies that it has contact with and aims to follow the 6 principles outlined within the UK Data Protection Act 2018 and the UK General Data Protection

Regulation (GDPR).

2. The Data Protection Principles

Personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject;

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Legislative framework/related policies/documents

- Legislative framework includes:
- UK General Data Protection Regulation
- UK Data Protection Act 2018
- The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019
- The Human Rights Act 1998
- The Protection of Freedoms Act 2012

- Freedom of Information (Scotland) Act 2002
- Public Records Scotland Act 2011
- Related policies, procedures and documents include:
- Freedom of Information Policy
- Public Interest Disclosure (Whistle Blowing) Policy
- Information Security Policy
- Information Security Incident Management Procedure
- University Partnership IS Acceptable Use Policy
- Records Management Policy (including the UHI Records Retention Policy)
- Business Continuity Policy
- Staff Recruitment & Selection Policy
- Protecting Vulnerable Groups (PVG) Scheme procedure for New & Existing Staff Procedure
- Protecting Vulnerable Groups (PVG) Admissions & Student Funding Team Procedure
- Secure Handling, Use, Storage and Retention of Disclosure Information Procedure

3.1.21 DP Guidelines for Staff

4. Scope

- Information/data is legitimately gathered and processed for a variety of reasons including the recruitment and payment of staff; the recruitment of students; the payment of student bursaries and discretionary funds; the organisation and administration of courses and programmes; student prize giving and graduation ceremonies; the monitoring of health and safety arrangements; the monitoring of equality; diversity and inclusion strands (i.e. age, disability, gender, sexual orientation, race, ethnicity and religion) particularly in respect of student admissions/staff recruitment and the monitoring of performance; procurement of goods and services (including the payment of contractors); achievement and assessment and compliance with statutory obligations; Government agencies and other relevant bodies.

- The college is registered as a data controller with the Information Commissioner's Office and endeavors at all times to maintain data in secure conditions. A general outline of the personal data UHI Inverness processes has been notified to the Information Commissioner and can be viewed via the ICO register at www.ico.org.uk under registration number Z7631145.

- This Policy should be read in conjunction with other relevant documents and policies noted above in Section 3.

5. Responsibilities

- **The College Board of Management** are responsible for the approval of the Data Protection Policy; overseeing the monitoring the college's compliance with the GDPR; directing the EMT to take any action necessary to mitigate information risk(s) and data security risk(s) as notified to the Board and/or its sub-committees.

- **The College Principal & Chief Executive** has strategic responsibility for data protection and decision-making responsibility in relation to organisational risk(s) of a data protection and information security nature.

- **The College Executive Management Team** are responsible for providing leadership and commitment to the embedding of the data protection principles; ensuring action is taken (where required) to ensure compliance with the GDPR; and, on-going review of the Data Protection Policy.

- The Data Protection Officer is responsible for:

    - Review & revision of the Data Protection Policy and for ensuring
    - the associated data protection guidance for staff is regularly updated to ensure currency.

    - Maintaining an organisation wide register of all personal data processing activities, in accordance with Article 30 of the GDPR.

    - Maintaining a register of all Subject Access Requests and personal data released in accordance with Article 15 of the GDPR.

    - Developing and embedding organisational data sharing agreements, Controller/Processor and Controller/Controller processing agreements and maintaining a register of all current arrangements.

    - Providing advice (where sought) with regard to data protection impact
    - assessments and monitoring compliance with the controls introduced to mitigate risk.

    - Development & delivery of staff training on data protection matters;

    - Provision of advice & guidance to college staff at all levels (including the Board of Management) on data protection matters and compliance with associated legislation;

    - Acting as the Data Controller on behalf of the college which includes

- liaison with the ICO on matters relating to the processing of personal data and cooperating with the ICO as the Supervisory Authority;

- Monitoring & reporting to EMT, Audit Committee, F & GP Committee and Board of Management (as appropriate) regarding the college's compliance with current data protection legislation and any information risks giving cause for concern;

- **All managers** are responsible for ensuring:

- Development and on-going maintenance of a departmental personal data register which includes all areas under their control;

- The secure storage, access, control and management of the personal
- data processed within their functional area;

- Understanding their own personal responsibilities regarding the Information Asset Owner Guidelines;

- All staff they manage undergo training on data protection and
- information security on an annual basis.

- **All staff** are responsible for ensuring:

  - The security of the personal data that they process;

  - Compliance with both the data protection policy and the
  - associated staff guidelines;

  - Any suspected data breach is notified to the college Data Controller or
  - ICT Manager immediately they become aware of it;

  - Annual completion of the compulsory staff training modules on data protection and information security.

  - The information rights of data subjects as outlined in current legislation are respected and can be fully exercised.

6. Information Rights

Current legislation provides the following rights to all data subjects:

6.1 The right to be informed (how their personal data is processed).
6.2 The right to access (the right to be given a copy of their own data).
6.3 The right to have personal data corrected if believed to be inaccurate

6.4 The right to have their data deleted (in certain circumstances).
6.5 The right to limit how their data is used (in certain circumstances).
6.6 The right to data portability (in certain circumstance).
6.7 The right to object to data processing (in certain circumstances).
6.8 Rights regarding automatic decision making and profiling.

7. Compliance

- This policy will be audited regularly with reports going to the executive management team and Board of Management Audit Committee.

- Compliance with this policy is the responsibility of all college staff. Any deliberate breach of the data protection policy may lead to disciplinary action being taken or access to the college's facilities being withdrawn or even criminal prosecution. Any questions or concerns about the interpretation of this policy should be addressed to the college's Data Controller.

- Any member of staff, student or other individual who considers that the policy has been breached in respect of personal data about them, should raise the matter with the college's Data Controller.

- The Data Controller can be contacted by email: data.controller@inverness.uhi.ac.uk

- This policy does not form part of the formal contract of employment, but it is a condition of employment that employees abide by the policy and adhere to the guidelines which follow. Failure to adhere to the policy can therefore result in disciplinary proceedings.

8. Monitoring

- Appropriate procedures for monitoring and evaluation are the responsibility of the lead officer. These procedures will be subject to audit by the Quality Unit.

- The Data Controller will maintain statistical data regarding the number of enquiries and access to data requests. Such information will be reported to the Audit Committee on an annual basis.

9. Review

- This policy will be reviewed on a 3 yearly basis