

Data Protection Policy

Document Reference Number

Date Approved

Review Date

EIA

Lead Officer

Review Officer

PL/GO/2026/002

23/06/2026

23/06/2029

Yes

Principal & Chief Executive

Information Development Manager

Version Control History

Reviewer	Date of Change	Summary of Revisions made
Information Development Manager	27.11.09	Amendments approved by BoM Audit Committee
Information Development Manager	25.05.10	Review approved by BoM Audit Committee
Information Development Manager	24.11.15	Review Approved by BoM Audit Committee
Information Development Manager	19.09.17	Review Approved by BoM Audit Committee
Information Development Manager	30.06.20	Review Approved by BoM
Information Development Manager	Aug 2023	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.
Information Development Manager	March 2026	Update to include new legislative reference. Some language amendments made but context remains unchanged.

Contents

1. Policy Statement.....	3
2. The Data Protection Principles	3
3. Legislative Framework / Related Policies	4
4. Scope	4
5. Responsibilities.....	5
6. Information Rights	7
7. Compliance.....	7
8. Monitoring.....	8
9. Review.....	8

1. Policy Statement

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

UHI Inverness 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, the UK General Data Protection Regulation (GDPR) and the Data Use and Access Act 2025.

2. The Data Protection Principles

2.1. 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 is inaccurate regarding the purposes for which it is processed, is 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

- 3.1. Publicly available UHI Inverness policies and procedures can be accessed via our website: [About us – Publications](#). Staff and Board Members can access the full range of internal policies and procedures through the Quality SharePoint site.
- 3.2. Legislative framework includes
 - 3.2.1. UK General Data Protection Regulation
 - 3.2.2. UK Data Protection Act 2018
 - 3.2.3. The Data Use and Access (DUAA) Act 2025
 - 3.2.4. The Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019
 - 3.2.5. The Human Rights Act 1998
 - 3.2.6. The Protection of Freedoms Act 2012
 - 3.2.7. Freedom of Information (Scotland) Act 2002
 - 3.2.8. Public Records Scotland Act 2011
- 3.3. Related policies, procedures and documents include:
 - 3.3.1. Freedom of Information Policy
 - 3.3.2. Public Interest Disclosure (Whistle Blowing) Policy
 - 3.3.3. Information Security Policy
 - 3.3.4. Information Security Incident Management Procedure
 - 3.3.5. University Partnership IS Acceptable Use Policy
 - 3.3.6. Records Management Policy (including the UHI Records Retention Policy)
 - 3.3.7. Business Continuity Policy
 - 3.3.8. Staff Recruitment & Selection Policy
 - 3.3.9. Protecting Vulnerable Groups (PVG) Scheme procedure for New & Existing Staff Procedure
 - 3.3.10. Protecting Vulnerable Groups (PVG) Scheme Procedure for Students
 - 3.3.11. Secure Handling, Use, Storage and Retention of Disclosure Information Procedure
 - 3.3.12. DP Guidelines for Staff

4. Scope

- 4.1. 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.

- 4.2. UHI Inverness is registered as a data controller with the Information Commission (IC) and endeavours 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 Commission and can be viewed via the register at www.ico.org.uk under registration number Z7631145.
- 4.3. This Policy should be read in conjunction with other relevant documents and policies noted above in Section 3.

5. Responsibilities

- 5.1. **The Board of Management** are responsible for the approval of the Data Protection Policy; overseeing the monitoring UHI Inverness'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.
- 5.2. **The 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.
- 5.3. **The Executive Management Team** are responsible for providing leadership and commitment to the embedding of the data protection principles; monitoring compliance with the UK GDPR and ensuring action is taken (where required) to ensure legal compliance with the data protection and associated legislation; and on-going review of the Data Protection Policy.
- 5.4. **The Data Protection Officer** is responsible for:
- Review & revision of the Data Protection Policy and ensuring
 - the associated data protection guidance for staff are 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 UHI Inverness which includes liaison with the IC on matters relating to the processing of personal data and cooperating with the IC as the Supervisory Authority;
- Upholding data subject's information rights and processing information rights requests within legal timescales;
- Monitoring & reporting to EMT, Audit Committee, F&GP Committee and Board of Management (as appropriate) regarding compliance with current data protection legislation and any information risks giving cause for concern.

5.5. **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.

5.6. **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 Data Controller or ICT Manager immediately when 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;

- Ensuring the departmental data register is updated to record any personal data processing being undertaken, to ensure it remains both current and accurate.

6. Information Rights

- 6.1. Current legislation provides the following rights to all data subjects:
- 6.1.1. The right to be informed (how their personal data is processed).
 - 6.1.2. The right to access (the right to be given a copy of their own data).
 - 6.1.3. The right to have personal data corrected if believed to be inaccurate
 - 6.1.4. The right to have their data deleted (in certain circumstances).
 - 6.1.5. The right to limit how their data is used (in certain circumstances).
 - 6.1.6. The right to data portability (in certain circumstance).
 - 6.1.7. The right to object to data processing (in certain circumstances).
 - 6.1.8. Rights regarding automatic decision making and profiling.

7. Compliance

- 7.1. This policy will be audited regularly with reports going to the executive management team and Board of Management Audit Committee.
- 7.2. 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 Data Controller.
- 7.3. 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 Data Controller.
- 7.4. Complaints or concerns regarding personal data processing or exercising one's information rights should be directed to the Data Controller who can be contacted by email: data.controller.ic@uhi.ac.uk and quality.ic@uhi.ac.uk ([About us - Complaints handling](#)).
- 7.5. 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

- 8.1. Appropriate procedures for monitoring and evaluation are the responsibility of the lead officer. These procedures will be subject to audit by the Quality Unit.
- 8.2. The Data Controller will maintain statistical data regarding the number of requests for personal data and information rights requests. Such information will be reported to the Audit Committee on an annual basis.

9. Review

- 9.1. This policy will be reviewed on a 3 yearly basis