

Data Protection Policy

Lead Officer (Post):	Vice Principal
Responsible Office/Department:	Senior Management Team (SMT) and Compliance
Responsible Committee:	Operations and Estates / SMT
Review Officer (Post):	Compliance Coordinator
Date policy approved:	28/04/2026
Date policy last reviewed and updated:	N/A
Date policy due for review:	02/04/2029
Date of Equality Impact Assessment:	N/A
Date of Privacy Impact Assessment:	N/A

Accessible versions of this policy are available upon request.

Policy Summary

Overview	This document will detail the 2026-2029 Data Protection Policy for UHI Shetland. This policy will demonstrate compliance with the UK GDPR and Data Protection Act (2018) and summarise the roles and responsibilities within the university around Data Protection.
Purpose	This policy sets out UHI Shetland's commitment to protecting personal data and complying with relevant legislation and describes how that commitment is implemented.

Scope	It applies to all personnel whether staff, contractor, other third parties, or members of partnership organisations with access to UHI Shetland data or information systems.
Consultation	Operations and Estates, Senior Management Group (SMG), Senior Management Team (SMT), Audit Committee
Implementation and Monitoring	This policy will be implemented in line with UHI Shetland policies and available to view on staff communication tools and will be monitored by the Compliance Coordinator and Senior Management Team.
Risk Implications	Failure to comply with the Data Protection Act (2018) and UK GDPR resulting in potential damage to reputation. Damage to trust from stakeholders, regulatory fines of other action, and/or compensation claims.
Link with Strategy	UHI Shetland's Data Protection Policy underpins the delivery of our Strategic Vision by ensuring that personal data is managed lawfully, securely and transparently across all areas of our work. By embedding clear responsibilities, robust governance and good data handling practice, the policy supports collaborative working, strengthens trust with our communities and partners, and enables ethical research, innovation and service delivery. It promotes sustainable and resilient organisational practice through responsible information management and staff development, helping UHI Shetland operate confidently at local, national and international levels.

1. Policy Statement

UHI Shetland has educational and business requirements to maintain certain personal data about living individuals in pursuit of its legitimate activities as a college and training provider.

UHI Shetland recognises that the correct and lawful treatment of personal data maintains confidence in the organisation and provides for successful operations.

Personal information, held in any form, is subject to the legal safeguards specified in the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and, where applicable, the EU GDPR. UHI Shetland fully endorses and adheres to the principles of the UK GDPR. These principles specify the legal conditions to be satisfied in relation to processing personal data.

Employees, students and any others who obtain, handle, process, transport and store personal data for UHI Shetland shall adhere to these principles.

2. Definitions

2.1 Act: Data Protection Act 2018

2.2 EU: European Union

2.3 UK GDPR: The General Data Protection Regulation (EU 2016/679) (GDPR) as retained and amended in UK law (UK GDPR)

2.4 GDPR: General Data Protection Regulation (EU) 2016/679 ICO Information Commissioner's Office

2.5 UHI: University of the Highlands and Islands

2.6 UK: United Kingdom

3. Purpose

- 3.1 This policy sets out UHI Shetland's commitment to protecting personal data and complying with relevant legislation and describes how that commitment is implemented.
- 3.2 UHI Shetland needs to process certain personal data relating to staff and students in order to fulfil its purpose and meet its legal obligations to funding bodies and the government.
- 3.3 UHI Shetland is committed to ensuring that personal data is collected, stored and disposed of in a secure and appropriate manner. We respect the data subject's right to privacy and accuracy, and their right to access their own personal data where appropriate.
- 3.4 UHI Shetland will process such information according to the Data Protection Principles that are set out in the UK GDPR and follows details guidance, regulations and frameworks issued by the relevant regulatory authorities.

4. Scope

- 4.1 All staff at UHI Shetland, including postgraduate students and researchers.
- 4.2 This policy applies to all persons, including employees, students, and others who obtain, handle, transport, store, or otherwise process personal data for, or under the auspices or instruction of, UHI Shetland.

5. Exceptions

There are no exceptions or exclusions to this policy.

6. Notification

This policy and attached procedures will be readily available on SH Staff Resources > Quality Matters > Policies and Procedures.

7. Roles and Responsibilities

7.1 Senior Management Team

Provide oversight and assurances that the College meets its obligation to inform individuals of data collection, processing, sharing and retention as set out in the 'right to be informed' provisions of the UK GDPR.

Provide oversight and assurances that the College meets its obligation to specify the purposes for which personal data is used.

Ensure that all people are treated justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

7.2 Compliance Coordinator

- Act as a single point of contact for all Data Protection issues at UHI Shetland and is the lead contact for the University's Data Protection Officer.
- Provide relevant data protection information to the UHI Head of Governance to enable them to comply with statutory reporting requirements (ICO).
- Maintain an up-to-date and accurate register entry with the Information Commissioner's Office (ICO) and pay the data protection fee to the ICO.
- Provide advice, training and guidance for all staff to ensure that the College collects and processes appropriate personal data only to the extent that it is needed to fulfil operational or legal requirements.
- Provide advice, support and guidance to staff to ensure that the College maintains the currency of its personal data, including overseeing the maintenance of appropriate departmental retention schedules and deletion classifications.
- Take the appropriate technical and organisational security measures to safeguard personal data.
- Ensure that appropriate safeguards are in place for personal information being transferred outside the UK.

- Creation and maintenance of Records of Processing Activities (RoPA) describing purposes, categories of data subjects/data, recipients, retention periods and security measures for controller and processor roles. The RoPA is kept accurate through data-mapping and regular review.
- Creation and maintenance of clear privacy notices to staff, students, applicants, alumni, research participants, website/app users and visitors. The notices explain purposes, lawful bases, recipients, retention, transfers, rights and how to contact the DPO.
- Ensures that all Freedom of Information (FOI) requests and Subject Access Requests (SAR) are completed in a timely manner in line with regulations and best practice.
- Ensure that the rights of data subjects can be fully exercised under the Act, including:
 - the right to be informed that processing is being undertaken.
 - the right of access to one's personal information.
 - the right to prevent processing in certain circumstances, and:
 - the right to correct, rectify, block or erase information which is incorrect or unnecessary.

7.3 Line Managers

Line Managers shall ensure that all staff and contractors are adequately briefed and comply with this policy. Managers shall ensure that, where appropriate:

- documents containing personal information have appropriate classification applied.
- retention policies are applied to personal information held on file.
- FOI/SAR requests are completed in a timely manner in liaison with the UHI Shetland Compliance Coordinator.
- Liaison with the Compliance Coordinator around the creation, maintenance and accuracy of RoPAs, in keeping with the review process for RoPAs.

7.4 All Employees

Personnel responsible for managing and handling personal information shall follow good data protection practice and comply with this policy, in any cases of doubt staff will consult the UHI Shetland Compliance Co-ordinator.

All staff must complete the appropriate mandatory training: **Information Security and GDPR.**

8. Related Policies, Procedures, Guidelines, and Other Resources

UHI Shetland maintains a range of data protection procedures, guidance documents, compliance documents and templates to aid and monitor the UHI Shetland's compliance with data protection law. The documents are made available to staff through the UHI Shetland Staff Resources.

9. Legislative Framework

The General Data Protection Regulation (EU 2016/679) (GDPR) as retained and amended in UK law (UK GDPR). The EU General Data Protection Regulation (Regulation 2016/679 of the European Parliament and of the Council), the Data Protection Act 2018, Privacy and Electronic Communications Regulations (PECR)

10. Version Control and Change History

Version	Date	Approved by	Amendment(s)	Author
0	28/04/26	SMT	New Policy	Vice Principal Operations