University of the Highlands and Islands

Data Protection Policy

POL013

Lead Officer (Post):	University Secretary
Responsible Office/ Department:	Principal and Secretary's Office
Responsible Committee:	Finance and General Purposes Committee
Review Officer (Post):	Director of Corporate Governance (Deputy Secretary); Data Protection Officer
Date policy approved:	17/08/2011
Date policy last reviewed and updated:	09/06/2022
Date policy due for review:	09/06/2024
Date of Equality Impact Assessment:	Click or tap to enter a date.
Date of Privacy Impact Assessment:	Click or tap to enter a date.

Accessible versions of this policy are available. Please contact the University Governance team.

Policy Summary

Overview	**To 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 the university'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 data or information systems.
Consultation	Head of Governance and Records Management and relevant committees to be consulted. UHI partners to be notified of change.
Implementation and Monitoring	Data Protection Officer, Head of Governance and Records Management, Head of Internal Audit – resources may be required to implement some elements. HGRM and HoIA aware of this.
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	How is this policy linked to University strategy?
Impact Assessment	Equality Impact Assessment:
	Privacy Impact Assessment:

1. Policy Statement

The University of the Highlands and Islands ("the university") has educational and business requirements to maintain certain personal data about living individuals in pursuit of its legitimate activities as a university. The university 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. The university 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 the university shall adhere to these principles.

2. Definitions

Act	Data Protection Act 2018
EU	European Union
UK GDPR	the General Data Protection Regulation (EU 2016/679) (GDPR) as retained and amended in UK law (UK GDPR)
GDPR	General Data Protection Regulation (EU) 2016/679
ICO	Information Commissioner's Office
UHI	University of the Highlands and Islands
UK	United Kingdom

3. Purpose

This policy sets out the university's commitment to protecting personal data and complying with relevant legislation and describes how that commitment is implemented.

4. Scope

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, the university.

5. Exceptions

This policy applies without exceptions, exclusions, or restrictions.

6. Notification

UHI partner organisations. This policy will be published on UHI's SharePoint area to all Academic Partners and staff.

7. Roles and Responsibilities

Ownership:

The University's Data Protection Officer (DPO) and Director of Corporate Governance (DoCG) will:

- Review this policy and make updates to reflect changes to legislation, case law, or best practice
- Ensure that adequate data protection procedures are available to staff

- Make online and face-to-face training available to all staff. The DPO will deliver training sessions for departments on request.

Compliance:

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

• documents containing personal information have appropriate classification applied

• retention polices are applied to personal information held on file

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 their Data Protection Officer.

8. Procedures

The Data Protection Officer and Director of Corporate Governance will audit and record the university's compliance with data protection law and best practice using the ICO's data protection Accountability Framework. The DPO and DoCG will make plans to continuously improve and will use the Accountability framework to guide this progress.

The Data Protection Officer and Director of Corporate Governance will maintain a range of data protection procedures, guidance documents, compliance documents and templates to aid and monitor the University's compliance with data protection law. These documents will cover:

- Privacy notices
- Legitimate Interest Assessments
- Data sharing agreements
- Safely sharing and storing information
- Data breaches
- Rights requests
- Data Protection Impact Assessments
- Due diligence
- International transfers
- Photography and recordings
- Registers of processing activity

The DPO and DoCG will contribute to university policies and action plans regarding records management and information security.

The university shall:

• 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;
• Ensure that any changes are notified to the ICO within appropriate timescales;
• Ensure that there is someone with specific responsibility for Data Protection;
• Observe fully the conditions regarding the fair collection and use of personal data;
• Meet its obligations to inform individuals of data collection, processing sharing and retention as set out in the 'right to be informed' under the UK GDPR;
• Meet its obligations to specify the purposes for which personal data is used;
• Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
• Ensure the quality of personal data used;

• Apply strict checks to determine the length of time personal data is held;
• Ensure that the rights of individuals about whom the personal data is held can be fully exercised under the Act and under the UK General Data Protection Regulation;
• 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;
• Ensure that the rights of people, about whom information is held, can be fully exercised under the Act (These include: 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);
• Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

9. Policy Detail

The policy is based on the principles set out in the UK GDPR, and follows detailed guidance, regulations and frameworks issued by the relevant regulatory body.

10. Risk Assessment

UHI's DPO will monitor compliance with DP law using the ICO's Accountability Framework and will report the following to UHI twice per year:

- Accountability tracker changes
- Number of data breaches and number, reportable breaches and a narrative explaining any patterns in breaches and improvements or issues.
- Registers of Processing Activity progress and outstanding issues in those registers.

11. 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).

12. Related Policies, Procedures, Guidelines and Other Resources

UHI maintains a range of data protection procedures, guidance documents, compliance documents and templates to aid and monitor the university's compliance with data protection law including those listed in section 8 of this policy. The documents are made available to staff through the UHI DP Advice SharePoint page.

13. Version Control and Change History

Version	Date	Approved by	Amendment(s)	Author
0	28/05/2018	HGRM	Updated slightly for post-GDPR use	(edited by DPO)
1	14/06/2022	DoCG	Updated in keeping with UHI DP progress and legislative changes	(edited by DPO)
2				
3				
4				