Data Protection Policy

Appropriate consultation undertaken	Yes ☒ No ☐
Impact on other policies considered	Yes ☒ No ☐
Equality Impact Assessment completed	Yes ☐ No ☒
Public Facing	Yes ☒ No ☐

Policy Owner	Head of HR & OD
Date first approved by SMT	28th August 2023
Date first approved by BoM	
BoM Committee	Human Resources
Date current version approved by SMT	May 2018
Date current version approved by BoM	24th May 2018
BoM Committee	Human Resources

Review period	3 years
Date of last review	August 2023
Date of next review	August 2026

Data Protection Policy

1. Policy Statement

UHI Argyll (the "College") has educational and business requirements to maintain certain personal data about living individuals in pursuit of its legitimate activities as a College and, as a partner in the University of the Highlands and Islands.

We recognise 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. We fully endorse and adhere 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 must 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 College's commitment to protecting personal data and complying with relevant legislation and describes how that commitment is implemented. It summarises the roles and responsibilities within the College and outlines the support provided by the partnership's shared Data Protection Officer, James Nock.

4. Scope

This policy applies to all employees, students, and other third parties who collect, handle, transport, store, or otherwise process personal data for, or under the auspices or instruction of, the College.

5. Roles and Responsibilities

The University's (shared) **Data Protection Officer** and Director of Corporate Governance will review and maintain this policy including any associated resources.

This will include:

- Reviewing this policy and its associated resources and procedures and making updates to reflect changes to legislation, case law, and best practice;
- Ensuring that adequate data protection procedures are available to staff;
- Making online and face-to-face training available to all staff. The DPO will deliver training sessions for departments upon request.

Line Managers are responsible for ensuring that all staff and contractors are adequately briefed and comply with this policy.

Departmental Managers are responsible for ensuring that, where appropriate:

- Personal information is safely and securely stored, and:
- Retention classifications are properly applied to personal information held on file

All employees must:

- manage, handle or process personal information in line with this policy and guidance.
- Complete the appropriate mandatory training modules (every 2 years):
    - Information Security
    - Data Protection/GDPR

Any employee who is unsure should consult with the Head of HR&OD, who is the College's Single Point of Contact (SPOC) for data protection issues. The Data Protection Officer can also provide professional support and advice in all data protection matters.

The **Head of HR&OD** will:

- Act as a single point of contact for external communications and is the lead contact for the University's (shared) Data Protection Officer.
- Provide relevant data protection information to the Governance Officer 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:
- Ensure that any changes are notified to the ICO within appropriate timescales:

- 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.

- 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;

- 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);

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

Procedures – The Key Things You Need to Know

1. Resources and Procedures

The UHI Data Protection Team maintains a range of data protection procedures, guidance documents, compliance documents and templates to aid and monitor the university partnership's compliance with data protection law – you can access these here.

2. Subject Access Requests

All explicit (or potential) requests for personal data must be referred immediately to the Head of HR&OD, who will respond in line with the regulatory and statutory requirements, seeking advice from the Data Protection Officer, where appropriate.

3. Data Breaches

All confirmed or suspected data breaches must be referred to the Head of HR&OD AND the Data protection Officer immediately:

dataprotectionofficer@uhi.ac.uk

The Head of HR will respond in line with regulatory and statutory requirements, seeking advice from the Data Protection Officer.

4. Safely sharing and storing information

You must no longer use paper versions of documents containing personal information unless exceptional circumstances apply. You must ensure that any such records are digitised into a secure SharePoint location as soon as possible and that paper versions are securely disposed of as soon as is practicable.

Departmental Managers must ensure that digital information is retained securely on SharePoint, in line with the College's Document Retention Schedule and in line with the UHI deletion classifications to ensure currency.

5. Data Sharing Agreements (DSAs).

Any employee considering the sharing of personal data must ensure that the activity is covered by an existing DSA. If in doubt, you must consult with the Head of HR&OD or the Data Protection Officer to seek advice about whether it is appropriate to set up a new data sharing agreement.

All data sharing agreements must be retained centrally by the Head of HR&OD.

6. Privacy Notices

Privacy notices are required in all cases where we are collecting personal data from or about individuals (data subjects). You must consult with the HR&OD or the Data Protection Officer where you identify a *potential* requirement for a privacy notice.

7. Data Protection Impact Assessments (DPIAs)

A DPIA is required for any new information process. The Data Protection Officer can provide support and advice if you need to undertake an assessment.

8. International Data transfers

You must consult with the Data protection Officer if you plan to transfer any personal data outwith the EU.

9. Photography and video recordings

This is restricted to authorised employees (Marketing) and subject to an appropriate privacy notice. You must not use photography or video recordings without first consulting with the Data Protection Officer.

10. Registers of processing activity

Currently under development.

11. Legitimate Interest Assessments (LIAs)

You must seek the approval of the Head of HR&OD prior to completing a LIA.

12. Risk Assessment

The Head of HR&OD will monitor compliance with DP law using the ICO's Accountability Framework and will report the following to the Board of Management annually:

- 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.

13. 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).