

Data Protection Policy

Version Control History

Version Number	Date of Change	Summary of Revisions Made
3	July 2015	Scheduled revision. Changes to job titles and responsibilities in section 5 of the Policy, and inclusion of Heads of Research Centre in relation to personal data related to research. Not seen at CMT but approved by QM and notified to CMT 6 March 2013.
3.1	July 2016	Footer updated to reflect new template model. Role title changed: International and Corporate Services Director, Vice Principal, Finance and Estates, Head of Quality.
3.2	November 2017	Cover date changed. Footers changed to update ownership and authorship. EIR Policy hyperlinked. Data Breaches procedure added in Staff Guidelines area.
3.3	December 2018	Footer updated to reflect changes to job titles and responsibilities. References to Data Protection Act 1998 replaced by General Data Protection Regulation (GDPR) and Data Protection Act 2018. References to Freedom of Information Officer and Data Protection Officer updated to Transitions Project Coordinator. Changes to job titles and responsibilities updated to reflect current organisational structure – Head of Student Experience, Student Records Manager, Student Services Manager, Quality Manager, Vice Principal External, Head of HR and OD, Chief Operating Officer. Hyperlinks updated to current version of documentation. References to the Office of the Information Commissioner updated to the Information Commissioner's Office (ICO). Removal of reference to charging element to subject access requests – this no longer applies under the new regulations. Reference to Student Journey added under 'Student Guidelines'.
3.4	March 2019	Footer updated to reflect changes to job titles and responsibilities.
3.4	March 2021	No updates to Policy
3.5	March 2023	Rebranded
4	February 2025	Complete re-write to bring in line with UHI policy, removal of guidance.

Data Protection Policy

1 Policy Statement and purpose

UHI Perth has educational and business requirements to maintain certain personal data about living individuals in pursuit of its legitimate activities as an FE College and also as part of the UHI Partnership.

UHI Perth 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 (DPA 2018), the UK General Data Protection Regulation (UK GDPR) and, where applicable, the EU GDPR. UHI Perth 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 Perth shall adhere to these principles.

UHI Perth 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.

2 Purpose

This policy outlines how UHI Perth will fulfil its obligations in accordance with the UK GDPR, the Data Protection Act 2018 and where applicable the EU GDPR.

UHI Perth needs to process certain personal data (see section 3 of this policy, Definitions) relating to staff and students in order to fulfil its purpose and to meet its legal obligations to funding bodies and the government.

UHI Perth will process such information according to the [Data Protection Principles](#) that are set out in the UK GDPR and follows detailed guidance, regulations and frameworks issued by the relevant regulatory authorities.

3 **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 UHI Perth

4 **Roles and Responsibilities**

Ownership: The UHI Perth Data Protection Lead, Director of HR and Organisational Development, Depute Principal Operations and the Data Protection Officer (DPO) 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 policies 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 the UHI Perth Data Protection Lead.

5 **Procedures**

The UHI Perth Data Protection Lead will audit and record UHI Perth's compliance with data protection law and best practice using the ICO's data protection Accountability Framework.

The UHI Perth Data Protection Lead will lead plans to continuously improve this area and will use the Accountability framework to guide this progress.

The UHI Perth Data Protection Lead will maintain a range of data protection procedures, guidance documents, compliance documents and templates to aid and monitor UHI Perth'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

UHI Perth 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

5 Risk Assessment

The UHI Perth Data Protection Lead will monitor compliance with Data Protection law using the ICO's Accountability Framework and will report the following to the Audit Committee of UHI Perth Board of Manager 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

6 Contact details

The Data Controller is UHI Perth.

Any Data Protection incidents should be reported to the UHI Perth Data Protection Lead who is the Clerk to the Board in the first instance via dataprotection.perth@uhi.ac.uk.

The UHI Data Protection Lead can also be contacted via telephone on 01738 877300 or by post to Clerk to the Board of Management, UHI Perth, Crieff Road, PERTH, PH1 2NX.

The Risk and Project Officer is responsible for monitoring the review of UHI Perth policies. This includes the ensuring that the policy and EQIA once approved are posted on the web.

7 Additional Guidance

All staff within UHI Perth can access the UHI data protection sharepoint area [UHI Data Protection Advice - Home](https://myuhi.sharepoint.com/sites/uhi-dp-02) (<https://myuhi.sharepoint.com/sites/uhi-dp-02>) which has resources and guidance notes that are relevant to all members of staff. They have been prepared to help staff work securely and keep personal data safe.