Data Protection Policy

December 2018

Also available in large print (16pt) and electronic format.

Ask Student Services for details.

www.perth.uhi.ac.uk

University of the Highlands and Islands
Perth College

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'.

Data Protection Policy

1 Purpose

The EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) came into force on 25 May 2018. They are concerned with the rights of individuals with regards to the processing of their personal data and their rights to gain access to personal information held about them by an organisation or individual within it, and the right to challenge the accuracy of data held. Individuals have a right to apply for access to information held about them by the College, or to information about a third party if they have appropriate permission to do so.

The terms of GDPR and the Act relate to data held in any form, including written notes and records, not just electronic data.

The College 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 Scope

This policy outlines how the College will fulfil its obligations in accordance with the General Data Protection Regulation and the Data Protection Act 2018. The College 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. The College will process such information according to the Data Protection Principles that are set out in by GDPR and the DPA.

3 Definitions

Personal data is identified by the College under the following terms:

Photographs, written personal details, video recordings, audio recordings, and any combination of items that can be assembled to identify an individual.

Classes of information currently held by the College may include:

- Personal details.
- Family, lifestyle and social circumstances.
- Education and training details.
- Employment details.
- Financial details.
- Goods or services provided.
- Racial or ethnic origin.
- Trade union membership.
- Physical or mental health or condition.
- Offences (including alleged offences).

GDPR and the DPA defines both personal data and sensitive personal data. Data processors must ensure that the necessary conditions are satisfied for the processing of personal data and in addition that the extra, more stringent, conditions are satisfied for the processing of sensitive personal data.

Personal data has a wide ranging definition and can include not only items such as home and work address, age, telephone number and schools attended but also photographs and other images.

Sensitive personal data consists of racial or ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and criminal record.

For further definitions, see the Data Protection Glossary.

4 Key Principles

The College will process all personal data according to the 6 principles of the Data Protection Act.

College Data Areas as defined in Section 5 will be responsible for the following aspects of data protection, which are regarded as essential for data integrity and security:

- Awareness of the 8 principles as detailed in the guidelines and in the act.
- Suitability of storage facilities.
- Retention and deletion of records.
- External disclosure and sharing procedures.
- Knowledge of GDPR subject access data request procedures.
- Review of local information policy.
- Clearly defined roles and responsibilities.
- Data breach reporting.
- Knowledge of data sharing arrangements (eg with UHI).
- How to deal with Freedom of Information Requests. FOI Staff Leaflet].

5 Responsibilities

The College, as Data Controller, is responsible for all Data Protection policies and procedures. Any Data Protection incidents should be reported to the Transitions Project Coordinator. The named Data Controller contact for the College is:

The Transitions Project Coordinator (foi.perth@uhi.ac.uk).

The following members of staff have responsibility for overseeing day-to-day data processing activities in the following data areas:

- College Principal/Senior Management Team (high level College strategy and finance).
- Head of Student Experience (central College information systems).

- Head of Human Resources and Organisational Development (staff records, training and development).
- Vice Principal, External (International student records).
- Head of Information Services (IT systems and security, library records, procurement).
- Sector Development Directors (Personal Academic Tutor records).
- Chief Operating Officer (payroll, finance, estates).
- Director of the Centre for Mountain Studies (personal data contained within and related to research activities).
- All data processors are responsible for awareness of, and adherence to, relevant data protection policies, procedures and regulations.

The Quality Manager is responsible for monitoring the review of College policies. The Quality approval check of the final policy is the responsibility of the Quality Manager who will arrange for the policy to be posted on the web.

6 Linked Policies/Related Documents

ICO Register of Data Controllers
Perth College Model Publication Scheme (Freedom of Information (Scotland) Act 2002)

GDPR Subject Access Request Form

Freedom of Information Request Form

Perth College Environmental Information Regulations Policy

Perth College ICT Acceptable Use Policy

Perth College Records Management and Procedures Policy

GDPR Data Protection Subject Access Request Form (CCTV)

Data Protection Glossary

ICO CCTV Code of Practice

7 Relevant Legislation

Data Protection Act 2018

Freedom of Information (Scotland) Act 2002

Human Rights Act 1998

Data Protection Guidelines

December 2018

Also available in large print (16pt) and electronic format.

Ask Student Services for details.

www.perth.ac.uk

University of the Highlands and Islands
Perth College

Data Protection Glossary

This glossary explains some of the words and terms associated with data protection issues. Parts of this information have been taken from the glossary available on the UK Information Commissioner's Office (ICO) website.

Consent Forms

Consent forms are forms that are used to obtain the permission of the data subject for their personal information to be used for a particular purpose. A consent form must be used at the point of collection and explicitly mention the particular purpose for which the information is being collected.

Data Controller

A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

In the case of Perth College, the College is the data controller because it determines the purposes for which, and the manner in which, any personal information is processed or is going to be processed. This includes being responsible for destroying the information when it is no longer relevant. Individual members of staff, who process data on behalf of the College, are data processors.

The Data Controller contact for the College is the Transitions Project Coordinator.

Data Processor

A person, who processes personal information on a data controller's behalf. Anyone responsible for the disposal of confidential waste is also included under this definition.

In the case of the Perth College, a data processor is any person or organisation that processes data or disposes of confidential waste on behalf of the College.

Data Protection (DP) Principles

The Data Protection Act 2018 sets out 6 Data Protection Principles. In summary these state that personal information shall:

1 Be lawful, fair and transparent);
2 Be obtained for a specified, explicit and legitimate purpose and shall not be processed in any manner incompatible with that purpose;
3 Be adequate, relevant and not excessive for those purposes;
4 Be accurate and kept up to date;
5 Not be kept for longer than is necessary for that purpose;

6 Be kept safe from unauthorised access, accidental loss or destruction;

The GDPR includes a 7th Principle called the accountability principle. It states that data controllers shall:

7 Have appropriate measures and records in place to be able to demonstrate their compliance with the data protection principles.

Data Subject

This is the living individual who is the subject of the personal information (data).

Data Subject Access Request

See Subject Access Request.

European Economic Area (EEA)

The European Economic Area (EEA) consists of all the countries of the European Economic Union (EU) and Iceland, Liechtenstein and Norway.

Notification

Notification is the process by which a data controller's processing details are added to a register. Under the Data Protection Act every data controller who is processing personal information needs to notify unless they are exempt. Failure to notify is a criminal offence. Even if a data controller is exempt from notification, they must still comply with the data protection principles. Information Commissioner's Office (ICO) maintains a public register of data controllers. A register entry only shows what a data controller has told the Commissioner about the type of data being processed. It does not name the people about whom information is held.

Annually, the College will notify the ICO that personal data is being processed and give the classes of personal data that are processed by the College, the types of people whose personal data can be processed and the purposes for which the data is processed. Details of the College's notification may be viewed on the Data Protection Public Register on the ICO website.

Personal Data

Personal data means information about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession.

Within the College, personal data, sometimes also called personal information, is any information about a living individual that can be used, either on its own or in conjunction with other information held by the College or other information likely to come into the possession of the College, to identify that person. It includes any expression of opinion about an individual and any indication of the intentions of the College in respect of the individual. It includes information stored in any medium: paper and electronic, text, image, audio and visual.

Privacy Impact Assessment

Privacy Statements

Processing

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Processing of personal information includes collecting, using, storing, destroying and disclosing information.

Recipient

Recipient, in relation to personal data, means any person to whom data is disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of the data processor) to whom it is disclosed in the course of processing the data for the data controller. It does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law (eg Police enquiries).

Sensitive Personal Data

Sensitive personal data includes:

- The racial or ethnic origin of the data subject.
- Their political opinions/affiliations.
- Their religious beliefs (or beliefs of a similar nature).
- Whether they are a member of a Trade Union.
- Their physical or mental health or condition.
- Their sexual life/orientation.
- Genetic/biometric data.

Subject Access Request

Under the GDPR and DPA, individuals can ask to see all personal data held about them. If an individual wants to exercise this subject access right, they should submit a request to the person or organisation that they believe is processing the data.

A subject access request can be made verbally or in writing A request must include enough information to enable the person or organisation to satisfy itself as to the identity of the individual who is the data subject and to enable them to find the information.

A reply must be given within one month. A data controller should act promptly in requesting any further information necessary to fulfil the request. If a data controller is not processing personal information of which the individual is the data subject, the data controller must reply saying so.

In the case of the College, a GDPR subject access request should be made to the Transitions Project Coordinator. A request must be made in writing using the appropriate form; you can download the GDPR Subject Access Request form (Word) or get hard copies from College reception areas.

Third Party

Third party, in relation to personal data, means any person other than:

- The data subject.
- The College (the data controller).
- Any data processor or other person authorised to process data for the College or processor.

The expression third party does not include employees or agents of the data controller or data processor, who are treated as being part of the data controller or processor. Note that "third party" is different from "recipient", which effectively separates employees/agents of the data controller/processor from the data controller/processor itself.

Staff Guidelines

Staff should be aware who is responsible for Data Protection compliance issues within their department. Contacts are listed in the Data Protection Policy. You should be aware of the 8 Data Protection principles and be aware of how requests for information should be handled.

Your Rights

As for anyone whose personal data the College processes, you have the right to:

- Be informed what personal data about them the College holds and what it is used for.
- Access this personal data.
- Update the personal data the College holds.
- Be informed how the College is complying with its obligations under the Act.
- Complain to the Transitions Project Coordinator if you feel that the Data Protection policy has not been followed.

You will usually have access to your Human Resources (HR) records via an informal request to your head of Curriculum Area or Department, or to the Human Resources department.

If you wish to access your personal data under the provisions of the Data Protection Act, you should make a Data Subject Access Request.

Your Responsibilities

Providing Personal Data to the College

Like everyone who provides personal data to the College, you are responsible for ensuring adherence to the Data Protection Principles, especially with regard to accuracy. This means that you have a responsibility to ensure that personal data you provide to the College is accurate and up-to-date. The responsibility includes checking information that the College makes available via corporate systems or sends out from time to time showing your personal information that is being processed (ie stored).

Processing Personal Information on Behalf of the College

You are required to supervise students who process personal information as part of the course for which you are responsible and you must inform the College's Transitions Project Coordinator to ensure that the activity is covered by the College's registration with the Information Commissioner's Office.

Anyone who processes information about other people on behalf of the College (eg about students' course work, opinions about ability, references to other academic institutions, conference or visitor details, details of personal circumstances or research data) must comply with the Data Protection Principles and the College's ICT Acceptable Use Policy. Staff may find the guidance issued in the JISC Data Protection Guide, and the College Data Protection Guidelines a useful reference.

Data Security

Data should be secured appropriately according to its format. Manual records should be kept in locked containers, electronic information should be password protected and encrypted. Staff should be made aware of screen security, ie that personal information is not left on screens visible to third parties. Records should be disposed of securely; by shredding for manual records and by authorised disposal methods via the College IT team. Staff should not create new electronic or manual systems which contain personal data without consultation with the Transitions Project Coordinator.

Staff should not disclose personal data requested by any other party outwith the EEA without the specific and informed consent of the data subjects concerned.

Data Breaches

The college must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error.
- Unforeseen circumstances such as a fire or flood.
- Hacking attack.
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

However the breach has occurred, there are four important elements to any breach management plan:

- Containment and recovery.
- Assessment of ongoing risk.
- Notification of breach.
- Evaluation and response.

Any member of staff who suspects, or knows, that data has been used unlawfully or without the authority of the college, should contact the Transitions Project Coordinator:

Kirsty Campbell
foi.perth@uhi.ac.uk
01738 877625

If the breach contains data of university HE students, the University Head of Governance and Records Management should also be contacted:

Roger Sendall
roger.sendall@uhi.ac.uk

Student Guidelines

Your Rights

As for anyone whose personal data the College processes, you have the right to:

- Be informed what personal data about you the College holds and what it is used for.
- Access this personal data.
- Update the personal data held.
- Be informed how the College is complying with its obligations under the Act.
- Complain to the Transitions Project Coordinator if the Data Protection policy has not been followed.

If you want to look at and check the accuracy of your personal data held centrally, you can access your student record via www.studentjourney.ac.uk.

If you wish to access your personal data under the provisions of GDPR the Data Protection Act, you should make a data GDPR Subject Access Request.

Your Responsibilities

Providing Personal Data to the College

Students must ensure that all personal data provided to the College is accurate and up to date. Changes of address, corrections to contact details etc are to be notified immediately to the Student Records team or by accessing and updating records via www.studentjourney.uhi.ac.uk.

Processing Personal Information

Under GDPR and the Data Protection Act and the College's Data Protection Policy students have responsibilities when processing personal data. These include:

- Students who are considering processing personal data as part of their studies must notify and seek approval from their supervisor before any processing takes place.
- Students who are processing personal data other than as part of their studies should contact the ICO to ensure that they are doing so in compliance with GDPR and the Data Protection Act 2018 as they will not be covered under the College's registration.

CCTV

The College adheres to the ICO CCTV Code of Practice, which lays out guidelines for use, signage and access to CCTV footage.

Where CCTV is used in the College, there are appropriate signs which give information about purpose, the Data Controller and contact details. Requests for access to footage should be made via a GDPR Subject Access Request Form (CCTV).

Any queries about CCTV should be directed at the Transitions Project Coordinator in the first instance foi.perth@uhi.ac.uk.

Contact Details

The Data Controller is Perth College UHI.

The College Transitions Project Coordinator currently has responsibility for data protection and freedom of information for the College. Data protection and Freedom of Information queries should be addressed to the Transitions Project Coordinator, who can be contacted by telephone at 01738 877625 or by email at foi.perth@uhi.ac.uk.

Postal address:

Kirsty Campbell
Transitions Project Coordinator
Perth College
Crieff Road
PERTH
PH1 2NX