University of the Highlands and Islands
West Highland College
Oilthigh na Gàidhealtachd agus nan Eilean
Colaiste na Gàidhealtachd an Iar

Data Protection Policy

ELT manager	Vice Principal Academic Affairs
Responsible officer	Head of Student Support
Date first approved by BoM	March 2013
Date review approved by BoM	28 June 2017
Next Review Date	December 2019 or sooner if required through legislation
Equality impact assessment	8th August 2017
Further information (where relevant)	This policy is in line with legislation and any legislative changes will result in policy review out with the scheduled dates.

Reviewer	Date	Review Action/Impact	BoM

Contents

1.0 Introduction

1.1 West Highland College UHI recognises that information systems, both electronic and manual, their associated processing tools and services and the information they contain are an integral part of teaching, learning and administration and are of vital importance to ensure that the organisation functions efficiently.

1.2 The College is committed to ensuring that the processing of personal data is only undertaken in the legitimate operation of the College's business. The College will ensure that the eight principles on which the Data Protection Act 1998 (the Act) is based are made known to and observed by all staff members.

1.3 The College is committed to ensuring that this policy and any associated procedures will be updated to reflect any future legislative changes and updates in a timely manner.

2.0 Scope

2.1 Embedded within the Act are eight Data Protection Principles which must be followed. These eight Principles provide the following:

Principle 1
Personal data shall be processed fairly and lawfully. Schedule 2 of the Act provides that certain conditions must be met e.g.

(i) the data subject has given consent
(ii) the processing is necessary.

Principle 2
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4
Personal data shall be accurate and, where necessary kept up to date.

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for those purposes.

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under the 1998 Act.

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to personal data.

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and Freedoms of data subjects in relation to the processing of personal data.

2.2 This policy covers all data coming under the provisions of the Act and all persons in the college recording, accessing or using that data in any way.

3.0 Key Principles

The key principles that the College will use in meeting its obligations to Data Protection are:

Designated Data Protection Officer

(i) The College as a corporate body is the data controller under the Act and whilst the College Board of Management is therefore ultimately responsible the College has designated that the Student and Customer Services Manager will act in the capacity of Data Protection Officer.

(ii) The College endeavours at all times to maintain data in secure conditions and processes and discloses information in terms of its notification to the Data Protection Commissioner.

Data Subjects

All staff members, students and other individuals are entitled to know:

- what information the College holds and processes about them and why;
- how to gain access to it;
- how to keep it up to date; and
- what the College is doing to comply with its obligations under the 1998 Act.

The College through this Policy and the issue of further guidance when appropriate will ensure that staff students and other data subjects are notified of the above as appropriate.

Access to information

a) Staff members, students and other individuals have a right to a copy of the personal information the College holds about them either in electronic or manual form. The College may make a charge not exceeding £10 for the provision of this information.

b) The College will comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days unless there is good reason for delay. In the event of there being a delay, the delay will be explained in writing to the data subject making the request.

c) Parents or guardians of students aged over 16 do not have the right of access to information and will not be given access to data relating to the student unless the student has given written consent for the release of information

Objections to Data Processing

Staff, students and other individuals have a right to object to data processing that causes damage or distress. Any objection to processing must be made in writing to the college Designated Data Controller.

Accuracy of Data

a) Staff members are responsible for:
- (i) checking that the information they provide to the College in connection with their employment is accurate and up to date; and
- (ii) informing the College of any changes to the information they have provided.

b) Students are responsible for:
- (i) ensuring that all personal data provided to the College is accurate and up to date;
- (ii) notifying the College of any alterations to their address or personal details as provided on the enrolment form.

The College cannot be held responsible for any errors unless the member of staff or student has advised the College accordingly.

Processing of Data

a) Staff who, as part of their responsibilities, collect data about other people must comply with the College's guidelines.

b) Staff must ensure that any personal data is held securely and that information is not disclosed either orally or in writing or accidentally or otherwise to any third party.

c) Students using the College's computer facilities may, on occasion, process personal data as part of their studies. If they do so they must notify their tutor and be made aware of this policy and any procedures for dealing with data within the law.

Sensitive Data

In certain circumstances where data is deemed to be of a sensitive nature in terms of the Act, the College may only process personal data with the consent of the individual. Under the Act sensitive data would cover such areas as: information about a person's health, racial or ethnic origin, criminal convictions or trade union membership. The information may be processed to ensure the College is a safe place for everyone or in legitimate operation of other essential procedures, such as sick pay and in the monitoring of equal opportunities.

Assessment Data and Examination Results

a) Assessment grading and examination results will not be published on notice boards where a student can be identified by name; however, lists, using discreet individual SQA or other examining body reference may be used.

b) Results will not be divulged over the telephone unless there is prior written agreement to do so.

Retention of Data

a) The College will keep some forms of information for longer than others. In general, electronic information about students will be kept centrally by the Registry Department or in some cases as relevant by UHI Executive Office, for a period to comply with legal, funding and awarding body requirements and for general enquiries from past students about the education history.

b) The College will need to keep information about staff for longer periods of time. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

c) In certain circumstances, for example to comply with European funding requirements, the College may require to keep data for longer periods than noted above.

d) The College will develop a series of retention schedules for relevant individual departments to ensure compliance e.g. Finance, Student Services, Registry, Health & Safety.

Direct Marketing

Direct marketing is marketing to named individuals or to sole traders. It excludes marketing to businesses and other types of organisation. It covers the promotion of aims and ideals as well as the sale of products and services.

a) The College must have consent to send people marketing information, or to pass their details on to third parties.

b) The College must keep clear records to be able to demonstrate that consent was knowingly given. This marketing list will be compiled fairly and accurately, reflect peoples' wishes and will be kept up to date.

c) The College will use opt-in boxes when requesting consent. The statement to be used for both paper and electronic formats is as follows:

"Tick if you would like to receive further information about our courses or other services that may be of interest to you: by post □ / by email □ / by telephone □ / by text message □ / by recorded call □
The College will not share your details with any third parties for marketing purposes".

d) The College will not make marketing calls either in person or using pre-recordings to any number on the Telephone Preference Service (TPS) list without specific prior consent.

e) The College will not send marketing texts or emails to individuals without their specific prior consent.

f) Individuals can write at any time to object or opt-out from marketing messages. College electronic marketing messages will carry an opt-out option.

g) The College will only use direct marketing to those who have given knowing consent. It will not use third party lists.

CCTV

The College does not currently have any installed CCTV systems. However, in the event of any future installation the college would ensure that the following would apply:

a) The College will comply with the CCTV Strategy for Scotland, the requirements of the Data Protection Act and Human Rights Act in its use of surveillance systems. It will have a clear written procedure to guide users of the system and setting out the rights of those observed.

b) The College will operate a CCTV system for the purpose of preventing and detecting crime and for the protection and safety of its campus users. It would not use it for other purposes

c) The College would only introduce further surveillance cameras where no alternative option is available to meet the aim and where a privacy impact assessment has been completed. Final approval must be given by the Data Protection Officer and the designated senior manager, the Head of Student Support.

d) The use, purpose and extent of the CCTV system will be reviewed annually ensuring that its use continues to comply with the guiding principles within the CCTV Strategy for Scotland and the Data Protection Act.

Compliance

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken or access to College facilities being withdrawn or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer and/or the Head of Student Support.

Overriding Legislation

In the event of other legislation, for example the Adult Support and Protection Act 2007, requiring the release of data otherwise restricted under the Data Protection Act and that legislation overriding the Data Protection Act, then the College will comply with the overriding legislation. Any records of all such requests will be kept for information. Further, where there is a conflict in legislative requirements, the College will seek legal advice before making a decision whether or not to release data and will keep a record of that decision.

4.0 Responsibilities

4.1 The College Board of Management is responsible for ensuring the legal compliance of this policy.

4.2 The designated senior manager, the Head of Student Support is responsible for overseeing the work of the Data Protection Officer and ensuring compliance.

4.3 The Data Protection Officer is responsible for the implementation of this policy and to ensure that all staff, students and contractors comply with this policy and any related procedures.

4.4 Departmental and Course Area Leads are responsible for the application of the policy in all aspects of their teaching, and delivery

4.5 All staff members are responsible for complying with the principles of the Policy.

5.0 Related Documents

5.1 Data Protection Act (1998)
https://www.gov.uk/data-protection/the-data-protection-act

5.2 UHI Data Protection Policy and Procedures
https://www.uhi.ac.uk/en/about-uhi/governance/policies-and-regulations/data-protection/

5.3 Staff Disciplinary Policy and Procedure
http://staff.whc.uhi.ac.uk/Downloads/All-Policies/HR-Policies/Staff-Discipline-Policy.pdf

5.4 The UK Information Commissioner's Office provides a comprehensive guide to the data protection act on its website at https://ico.org.uk/

CCTV Strategy for Scotland
http://www.gov.scot/Publications/2011/03/18085554/0

ICO Direct Marketing
https://ico.org.uk/media/1555/direct-marketing-guidance.pdf

ICO In the picture: A data protection code of practice for surveillance cameras and personal information
https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

6.0 Review

6.1 This policy will be reviewed every 3 years or more regularly where dictated by legislative changes.