UHI | WEST HIGHLAND GÀIDHEALTACHD AN IAR

Data Protection Policy

ELT manager	Director of Finance & Resources
Responsible officer	Director of Finance & Resources
Date first approved by BoM	March 2013
Date review approved by BoM	24 June 2020
Next Review Date	April 2023 or sooner if required through legislation
Equality impact assessment	May 2020
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
DoFR	April 2020	Introduction expanded to include types of information the College collects and makes reference to the 7 principles under GDPR. Key principles have been separated out from Scope, which has been expanded to include link to ICO website and our registration number. Policy rewritten for GDPR.	

Contents

1.0 Introduction 3
2.0 Scope 3
3.0 Policy 3
3.1 Key Principles 3
3.2 Personal Information 4
3.3 Data Processing and the Lawful Basis 4
3.4 Individual Rights 5
3.5 Privacy Notices 6
3.6 Data Retention 6
3.7 Records of Processing Activities 7
3.8 Data Sharing 7
3.9 Transfers of Personal Data Outside the EU 7
3.10 Data Protection Impact Assessments and Data Protection by Design 7
3.11 Security and Personal Data Breaches 8
4.0 Responsibilities 8
5.0 Related Documents 9
6.0 Review 9

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 collects and uses information (data) about its staff, students and other individuals and bodies that it has contact with and follows the 7 principles outlined within the EU General Data Protection Regulations (GDPR).

1.3 The College is committed to ensuring that the processing of personal data is only undertaken in the legitimate operation of the College's business and will ensure that the 7 key principles lie at the heart of the College's approach to processing personal data.

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

2.0 Scope

2.0 This policy covers all data coming under the provisions of the GDPR and all persons in the college recording, accessing or using that data in anyway.

2.1 The college is registered as a data controller with the Information Commissioner's Office and endeavours at all times to maintain data in secure conditions. See https://ico.org.uk/ registrations number Z8275428

2.2 All staff are required to undertake mandatory Data Protection Training as part of their induction and as required updates/refresher training.

2.3 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 addressed to the Data Protection Officer.

3.0 Policy

3.1 Key Principles

Embedded within the EU General Data Protection Regulations are seven key principles which act as a guide for the college in all aspects of data processing. These are:

Principle 1
Personal data shall be processed fairly, lawfully and in a transparent manner in relation to individuals.

Principle 2
Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle 3
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

Principle 4
Personal data shall be accurate and, where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Principle 5
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguards the rights and freedoms of individuals.

Principle 6
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

Principle 7
The data controller shall be responsible for and be able to demonstrate compliance with these principles.

3.2 Personal Information

'Personal Data' includes information relating to natural persons who can be identified or who are identifiable either directly from the information by reference to an identifier (e.g. names, location data or an online identifier such as IP address) or indirectly from that information in combination with other information.

Personal data may also include special categories of personal data e.g. biometric data, genetic data, health details, racial or ethnic origin) or criminal conviction and offences data. These are considered to be more sensitive and may only be processed in more limited circumstances under Articles 9 and 10 of the GDPR.

3.3 Data Processing and the Lawful Basis

The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations

on the information or data, including retrieval, consultation, use and disclosure.

In order to process personal data, the college must have a valid lawful basis on which to do so. The lawful bases are as follows:

a) **Consent** – the individual has given clear consent for the processing of their personal data for a specific purpose.
b) **Contract** – the processing is necessary for a contract with the individual.
c) **Legal Obligation** – the processing is necessary to comply with the law.
d) **Vital Interests** – the processing is necessary to protect someone's life.
e) **Public Task** – the processing is necessary to perform a task in the public interest or for official functions and the task/function has a clear basis in law.
f) **Legitimate Interest** – the processing is necessary for the legitimate interests of the College or a third party unless there is good reason to protect an individual's personal data which overrides those legitimate interests.

3.4 Individual Rights

The college is aware of the following rights of individuals regarding the personal data held and is committed to upholding these rights:

Right to be informed
All individuals are entitled to know:

- What information the College holds and processes about them and why.
- How long it will be kept for.
- Who else it will be shared with.

This information should be provided in a privacy statement at the point the data is collected.

Right to access
All individuals have a right to obtain a copy of the personal information the College holds about them either in electronic or manual form. This is commonly referred to as subject access. The college has one month to respond and cannot charge a fee in most circumstances.

Right to rectification
Individuals have a right to have inaccurate personal data rectified or completed if it is incomplete. The request can be made either verbally or in writing and the college has one calendar month to respond to the request.

Right to erasure
This is also known as 'the right to be forgotten' and gives individuals the right to have personal data erased in certain circumstances. The request can be made either verbally or in writing and the college has one calendar month to respond to the request.

Right to restrict processing

Individuals have the right to request the restriction or suppression of their data in certain circumstances. If processing is restricted the college may store the data but not use it. The request can be made either verbally or in writing and the college has one calendar month to respond to the request.

Right to data portability
This allows individuals to obtain and reuse their personal data for their own purposes across different services. It only applies to information provided by the individual to the college.

Right to object
Individuals have the right to object to the processing of their personal data in certain circumstances. However, they have an absolute right to stop their data being used for direct marketing. Individuals must be made aware of their right to object. The request can be made either verbally or in writing and the college has one calendar month to respond to the request.

Rights related to automated decision-making including profiling
The right relates to automated decisions or profiling that could result in significant affects to an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision-taking based on sensitive data can only be done with explicit consent.

3.5 Privacy Notices

The college is required to provide individuals with a 'privacy notice' to inform them of how their personal data is used. The main privacy notices can be viewed here https://www.whc.uhi.ac.uk/about-us/data-protection/privacy-statements/

3.6 Data Retention

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed it will be disposed of securely. Paper records will be shredded or disposed of in confidential waste and electronic records will be permanently deleted.

The College will keep some forms of information for longer than others. In general electronic information about students will be kept for a period to comply with legal, funding and awarding body requirements and for general enquiries from past students about the education history.

The College may 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.

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

3.7 Records of Processing Activities

The college is required to keep a record of its data processing activities as a summary of the processing and sharing of personal information and the retention and security measures that are in place. Amongst other things this record contains details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU. These records can be found under Departmental Data Registers within the College Management Group information.

3.8 Data Sharing

Certain conditions would need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of the college. As a general rule personal data will not be passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible. Any transfers of personal data will meet the data processing principles as detailed in section 3.1, in particular it must be lawful and fair to the data subjects concerned. It will meet one of the lawful bases of processing as detailed in section 3.3. Legitimate reasons for transferring data would include:

- That is was a legal requirement
- It is necessary to provide services to its members

If no other conditions are met, then consent must be obtained from the individuals concerned and appropriate privacy notices provided.

The college must be satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely. Where a third party is processing personal data on behalf of the college, a written contract will be put in place.

3.9 Transfers of Personal Data Outside the EU

Personal data can only be transferred out of the European Union under certain circumstances. The GDPR lists the factors that would be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported. The college do not currently transfer data outside the EU.

3.10 Data Protection Impact Assessments and Data Protection by Design

It is particularly important to consider privacy issues when considering new processing activities or setting up new procedures or systems that involve personal data. Under GDPR, the college must undertake a Data Protection Impact Assessment for any processing that is likely to

result in a high risk to individuals.

GDPR imposes a specific 'data protection by design' legal requirement which means that data protection is integrated throughout processing activities and business practices from the design stages of a process and throughout the lifecycle. Therefore, the college will ensure that it has appropriate technical and organisational measures in place.

3.11 Security and Personal Data Breaches

The college is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The college will make every effort to avoid personal data breaches, however, in the event that there is a suspected data breach, in the first instance, this should be reported to the Data Protection Officer. The breach may need to be reported to the Information Commissioner's Office no later than 72 hours after the breach is discovered, if appropriate. Examples of personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction)
- Sending personal data to the incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission; and
- Loss of availability of personal data

If a breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the college will inform those individuals as soon as possible.

The college will keep a record of all personal data breaches, regardless of whether it is required to notify the Information Commissioner's Office. This record also records 'near misses' and is reported to each Audit Committee meeting.

4.0 Responsibilities

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

4.2 The Director of Finance & Resources has been designated as the Data Protection Officer and is also responsible for 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 Heads/Managers and Curriculum 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 (2018)
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

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/

6.0 Review

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