Humber Learning Consortium

Data Protection Policy

Version	3.1
Adopted	May 2019
Review	April 2020

Humber Learning Consortium (HLC) is committed to a policy of protecting the rights and privacy of individuals, including participants, staff and others, in accordance with Data Protection Law and the General Data Protection Regulation (GDPR) May 2018.

This policy applies to all HLC staff and those working on behalf of HLC.

Familiarity with the policy will help to ensure that all staff members understand their responsibilities and rights under Data Protection Law and the GDPR.

Prepared by
Humber Learning Consortium

Version: 3.1
Adopted: May 2019
Review: April 2020

DATA PROTECTION POLICY - INDEX

1. Purpose of the Policy

Humber Learning Consortium (HLC) is committed to a policy of protecting the rights and privacy of individuals, including participants, staff and others, in accordance with Data Protection Law and the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how organisations manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that HLC and its partners will need to be aware of as data controllers and processors, including provisions intended to enhance the protection of personal data.

HLC needs to process certain information about its staff and those working on our behalf through partnership arrangements, its participants and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.
2. The administration of programmes of study and courses.
3. Learner enrolment.
4. Examinations and external accreditation.
5. Recording learner progress, attendance and conduct.
6. Collection of financial information
7. Complying with legal obligations to funding bodies and government including local government.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) HLC must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

2. Compliance

This policy applies to all staff and participants (participants) of HLC and those working on behalf of through partnership arrangements. Any breach of this policy or of the Regulation itself will be considered an offence and disciplinary procedures will be invoked. As a matter of best practice, other agencies and individuals working with HLC and who have access to personal information, will be expected to read and comply with this policy. It is expected that those who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

3. Definitions

Personal Data is any data relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive data (Special categories of personal data) – is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Sensitive personal data (SPD) can be derived or inferred from non-SPD e.g. web browsing history of someone visiting a website whilst pregnant in and of itself is not SPD, but can infer pregnancy (which is SPD – data re: health condition).

Data subject – is a living individual

Controller – determines the purpose and manner of processing

Processor – performs actions on behalf of the controller

Processing – undertaking activities with the personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Breach notification - is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Data Protection Law – means Data Protection Act 2018 and General Data Protection Regulation

4. General Data Protection Regulation (GDPR)

The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

HLC are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information HLC collects and processes in accordance with the General Data Protection Regulation (GDPR).

Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.

The GDPR and this policy apply to all of HLC personal data processing functions, including those performed on participants, staff, suppliers and partner organisations personal data, and any other personal data the organisation processes from any source.

5. Responsibilities under the GDPR

HLC will mainly be a 'Controller' under the terms of the legislation – this means it is ultimately or jointly responsible for determining the purpose and manner of processing the data. HLC Funders will also have 'Controller' responsibility and in the main set the processing requirements that HLC and its Partners must follow. Partners for the most part will have 'Processor' responsibility and must fully understand, agree to and sign the HLC Data processing Agreement before commencing any processing of participant data.

HLC has appointed a Data Protection Officer (DPO), currently the MIS Manager who is available to address any concerns regarding the data held by HLC and how it is processed, held and used. HLC Chief Executive also oversees this policy.

This policy applies to all Staff and those working on or behalf of HLC. Any breach of the GDPR will be dealt with under HLC disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for HLC, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by HLC without having first entered into a data sharing or data processing agreement, which imposes on the third party obligations no less onerous than those to which HLC is committed, and which gives HLC the right to audit compliance with the agreement.

Partner organistaions that have a partnership agreement with HLC will have a named "Data Protection Officer" who will ensure partner compliance with HLC Data Protection, Data Processing, Information Security and Data Sharing Agreements.

Our data registration number is: Z7267594.

Staff and participants have a responsibility to

- Observe the Data Protection Principles as outlined below
- Ensure they have read, understand and accept any policies, procedures and guidance that relate to the processing of personal data (in all formats) and ensure its compatibility with the data protection principles
- Raise any concerns in respect of the processing of personal data with the Data Protection Officer
- Quickly ensure that any subject access requests and requests from third parties for personal data are passed to the Data Protection Officer
- Report any losses of unauthorised disclosures of personal data to the Data Protection Officer immediately.

Staff and participants must ensure that personal data they provide about themselves is accurate and kept up to date.

6. Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. HLC policies and procedures are designed to ensure compliance with the principles.

Personal data must be processed lawfully, fairly and transparently

Lawful basis for processing data must be sought before processing personal data. Lawful basis could be

- Consent
- Performance of a contract to which data subject is a party (or steps prior to it)
- Compliance with a legal obligation
- Vital interests of the data subject
- Public interest / public task (public authorities only)
- Legitimate interests

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources. The ICO provides guidance on 'Privacy notices and right to be informed' here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

HLC Privacy Notice is available here www.hlc-vol.org/privacy

The specific information that HLC will provide to the data subject must, as a minimum, include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the Data Protection Officer;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

Personal data can only be collected for specific, explicit and legitimate purposes
Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of HLC GDPR register of processing.

Personal data must be adequate, relevant and limited to what is necessary for processing
The Data Protection Officer is responsible for ensuring that HLC does not collect information that is not strictly necessary for the purpose for which it is obtained (refer to DPIA Tool GDPR REC for the Data flow/mapping).

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include an approved fair processing statement or link to privacy statement.

The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by owners to ensure that collected data continues to be adequate, relevant and not excessive

Personal data must be accurate and kept up to date with every effort to erase or rectify without delay
Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

It is also the responsibility of the data subject to ensure that data held by HLC is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

Staff should be required to notify HLC of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of HLC to ensure that any notification regarding change of circumstances is recorded and acted upon.

The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On an annual basis, HLC will review the retention dates of all the personal data processed, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Information Security and Data Retention Policies.

The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure). If HLC decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority.

The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
Personal data will be retained in line with the Data Retention Policy and, once its retention date is passed, it must be securely destroyed in line with Data retention and Information Security Policies.

Personal data must be processed in a manner that ensures the appropriate security
HLC will carry out a risk assessment taking into account all the circumstances of controlling or processing operations. In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or participants) if a security breach occurs, the effect of any security breach on HLC itself, and any likely reputational damage including the possible loss of trust.

The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)
The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility. HLC will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident management response plans. The ICO has published guidance on Accountability and Governance here https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

7. Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-making process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To request compensation if they suffer damage by any contravention of the GDPR.
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

HLC ensures that data subjects may exercise these rights:

Data subjects may make data access requests as described in Subject Access Request Procedure below.

Data subjects have the right to complain to HLC related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

8. Subject Access Requests

Individuals have a right to access any personal data relating to them which are held by HLC. Any individual wishing to exercise this right should apply in writing to the Data Protection Officer, details are available on HLC website.

Before processing this data the individual must provide identification evidence.

<u>Acceptable proof</u>

- Passport
- Driving license
- Birth Certificate (along with 1 of the following)
    - Bank Statement (within the last 3 months)
    - Utility Bill (within the last 3 months)

The procedure for subject access requests are as below

1. Data Subject should submit a written or emailed request for subject access or through the HLC Subject Access Request Form available to download from www.hlc-vol.org/privacy
2. They should provide valid proof of identity, acceptable forms as listed above
3. Subjects should provide as much information as they can to enable data to be located, i.e. name, address, date of birth, reference numbers
4. Signatures should be double checked against previously submitted documentation
5. Inform the Data Subject whether data is held about them
6. Ensure any third party individuals are not identified in collected data and take steps to prevent the disclosure such as a black marker pen.
7. Provide the Data Subject with a copy of the personal data which relates to the Data Subject together with an interpretation of any terms or codes used by HLC relating to the data.
8. Respond within 30 calendar days of completion of proof of identity.
9. Retain a copy of the information supplied (for use in case of the information being challenged.
10. Ensure a log of subject access requests has been made on the CRM.

Please note under the GDPR Article 12, that period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

9. Disclosure of Data

HLC undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police.

Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure.
- the disclosure is in the legitimate interests of HLC and the DS has been informed
- the disclosure is required for the performance of a contract.
- ensure third party individuals have been marked out of any disclosures.

In no circumstances will HLC sell any of its databases to a third party.

10. Security

Staff processing personal data should ensure that the data is secure: appropriate measures must be taken to prevent unauthorised access, disclosure and loss.

Specific security procedures and requirements are covered within HLC Information Security Policy.

11. Data Retention

Data retention periods are covered within HLC Data Retention Policy.

12. Breach Notification

HLC DPO should be informed immediately of a breach. It's vitally important that as much information as possible is provided to the DPO including:

- What data is involved?
- Was the data encrypted or otherwise protected?
- Who is affected, what type of information and how many records?
- How sensitive is the information?
- Are there any potential risks to individuals?
- What steps have already been taken to recover/locate the information?
- If items have been stolen provide the crime number.
- Details of how this happened and employees involved?
- Details of any ongoing, immediate risk to information security.

An internal investigation of events will immediately take place and an assessment made upon the seriousness of the event.

HLC has a responsibility to report a data breach to the supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it".

All breach notifications must be logged on HLC CRM System.

13. Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to Data Protection Law.

Please follow this link to the ICO's website www.ico.gov.uk which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact: The Data Protection Officer (DPO): privacy@hlc-vol.org

14. Policy Links

This policy should be considered in conjunction with the following policies and procedures:

- Information Security
- Data Sharing Agreement
- Data Processing Agreement
- Data Retention
- Recruitment and Selection Policy
- Grievance Procedure

15. Related Legislation

- The Freedom of Information Act 2000 (FOI Act)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)