Progressive, Innovative & Interactive Training

HCT Learning

Quality Assurance Manual

2020

Data Protection and Freedom of Information/GDPR

Table of Contents

1 Data Protection and Freedom of Information/GDPR

HCT Learning fully complies with all Data Protection Acts and ensures that all information collected on staff, trainers, clients and learners are used only for the purpose they have been originally collected. HCT Learning will ensure that their staff are fully trained in HCT Learning's policies regarding data protection. In addition, it will ensure that all staff members understand the terminology and requirements laid out under the Data Protection Act and that they understand their responsibilities in upholding these requirements.

1.1 Data Protection Policy

This document is provided in accordance with the Data Protection Act of 1998, and from the 25 May 2018, the EU General Data Protection Regulation 2016/679 (the GDPR) in relation to data protection. Clients are invited to read this policy on why and how we use your data and contact the office directly if they have any further questions.

Under GDPR guidelines HCT Learning agrees to the following:

- Obtain and process any collected and stored information fairly
- Keep data only for one or more specified and lawful purpose
- Use collected data only in ways which are compatible with the purposes for which the initial request was made
- Keep collected and stored data safe and secure
- Keep data accurate and up-to-date
- Ensure that the data collected is adequate, relevant and not excessive
- Retain data no longer than is necessary for the specified purpose or purposes
- Give a copy of their personal data, the reason it is being held, and a list of who has access to it, to any individual, upon written request

HCT Learning stores data both online and in hard copy. There is an internal web application to store all staff, client, trainer, learner and programme details. This system is called MyHCT. All the information contained on MyHCT is protected by the use of a secure log-in system. All members of staff have an individual password in order to login to the system. Access to personal protected information such as PPSN and DOB requires an extra password, therefore only users with permission can obtain the key information required. Our system has restricted, password protected access and meets global security encryption standards using a secure way of encrypting information. All hard copy assessment material is securely stored in a locked filing cabinet. These are destroyed six months after the certification period.

1.1.1 Disclosure to Third Parties

HCT Learning at times may be required to disclose information to third parties. HCT Learning specialises in offering part-time educational opportunities within the community, therefore much of the funding for its programmes arises from Community Employment Schemes. As a result, HCT Learning's learner data may arise, in part, from these types of third parties. This type of data can include personal details (names, PPS numbers and dates of birth), reasonable accommodation requirements, past education and work experience. HCT Learning in turn passes data such as assessment results and attendance back to the third parties. In order to certify a learner we need to share information with Lantra. This data may include the full name, address, date of birth, gender and photo identification of the learner. Photographic and video evidence generated as part of assessment on a programme may be shared with an External Authenticator for authentication of results as part of the certification process. HCT Learning has invested in an accountancy package (Sage), in order for us to complete our end of year accounts. As a result clients/learners contact details, programmes delivered and monies spent are inputted into this system. Some elements of this information will be required to be sent to our accountant at the end of the year in order to complete our end of year accounts. Sage is secure and only available on one computer within the office and has password protection to ensure that information is kept safe. The data sharing platforms which are used vary between third parties, each of which have highly secure password protected applications.

1.1.2 The Right To Be Informed

In order to keep clients/learners informed about how we use your data, the Data Protection Acts are live on our website. Learners will be informed in the information booklets and during induction. If anything changes we will contact the learner directly to inform them.

1.1.3 Provided to learners

You have the right to know the following information:

- the types of data we hold and the reason for processing the data
- our legitimate interest for processing it
- details of who your data is disclosed to and why
- how long we keep your data for, or how we determine how long to keep your data for
- where your data comes from
- your rights as a data subject
- your absolute right to withdraw consent for processing data where consent has been provided and no other lawful reason for processing your data applies
- your right to make a complaint to the Data Protection Commission if you think your rights have been breached
- whether we use automated decision making and if so, how the decisions are made, what this means for you and what could happen as a result of the process
- the name and contact details of our point of contact for data protection

1.1.4 The Right To Access

You have the right to access your personal data which is held by us. You can find out more about how to request access to your data by reading our Subject Access Request policy.

1.1.5 The Right To 'Correction'

If you discover that the data we hold about you is incorrect or incomplete, you have the right to have the data corrected. If you wish to have your data corrected, you should complete the Data Access Request Form which is located on the website or you can call the office.

Usually, we will comply with a request to rectify data within one month unless the request is particularly complex, in which case we may write to you to inform you that we require an extension to the normal timescale. The maximum extension period is two months.

You will be informed if we decide not to take any action as a result of the request. In these circumstances, you are entitled to complain to the Data Protection Commission and have access to a judicial remedy.

Third parties to whom the data was disclosed will be informed of the rectification.

1.1.6 The Right To 'Erasure'

In certain circumstances, we are required to delete the data we hold on you. Those circumstances are:

- where it is no longer necessary for us to keep the data
- where we relied on your consent to process the data and you subsequently withdrew that consent. Where this happens, we will consider whether another legal basis applies to our continued use of your data
- where you object to the processing (see below) and the company has no legitimate interest to continue the processing
- where we have unlawfully processed your data
- where we are required by law to erase the data

If you wish to make a request for data deletion, you should complete the Data Access Request Form which is located on the website or you can call the office.

We will consider each request individually, however, you must be aware that processing may continue under one of the permissible reasons. Where this happens, you will be informed of the continued use of your data and the reason for this.

Third parties to whom the data was disclosed will be informed of the erasure where possible unless to do so will cause a disproportionate effect on us.

1.1.7 The Right To 'Restriction'

You have the right to restrict the processing of your data in certain circumstances.
We will be required to restrict the processing of your personal data in the following circumstances:

- where you tell us that the data it holds on you is not accurate. Where this is the case, we will stop processing the data until it has taken steps to ensure that the data is accurate
- where the data is processed for the performance of a public interest task or because of our legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst we consider whether our legitimate interests mean it is appropriate to continue to process it
- when the data has been processed unlawfully

- where we no longer need to process the data but you need the data in relation to a legal claim.

If you wish to make a request for data restriction, you should complete the Data Access Request Form which is located on the website or you can call the office.

Where data processing is restricted, we will continue to hold the data but will not process it unless you consent to the processing or processing is required in relation to a legal claim.

Where the data to be restricted has been shared with third parties, we will inform those third parties of the restriction where possible unless to do so will cause a disproportionate effect on us.
You will be informed before any restriction is lifted.

1.1.8 The Right To Data 'Portability'

You have the right to obtain the data that we process on you and transfer it to another party. Where our technology permits, we will transfer the data directly to the other party.
Data which may be transferred is data which:

- you have provided to us; and
- is processed because you have provided your consent or because it is needed to perform the contract between us; and
- is processed by automated means

If you wish to exercise this right, please contact HCT Learning to speak with the point of contact for data protection.

We will respond to a portability request without undue delay, and within one month at the latest unless the request is complex or we receive a number of requests in which case we may write to you to inform you that we require an extension and reasons for this. The maximum extension period is 2 months.

We will not charge you for access to your data for this purpose.
You will be informed if we decide not to take any action as a result of the request, for example, because the data you wish to transfer does not meet the above criteria. In these circumstances, you are able to complain to the Data Protection Commission and have access to a judicial remedy.

The right to data portability relates only to data defined as above. You should be aware that this differs from the data which is accessible via a Subject Access Request.

1.1.9 The Right To 'Object'

You have a right to require us to stop processing your data; this is known as data objection.

You may object to processing where it is carried out:

- in relation to the company's legitimate interests
- for the performance of a task in the public interest
- in the exercise of official authority; or
- for profiling purposes

If you wish to object, you should do so by completing the Data Access Request Form which is located on the website or you can call the office.

In some circumstances we will continue to process the data you have objected to. This may occur when:

- we can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights; or
- the processing is required in relation to legal claims made by, or against, us.

If the response to your request is that we will take no action, you will be informed of the reasons.

1.1.10 Right Not To Have An Automated Decision Made About You

You have the right not to have decisions made about you solely on the basis of automated decision making processes where there is no human intervention, where such decisions will have a significant effect on you.

However, HCT Learning does not make any decisions based on such processes.

We may carry out automated decision making with no human intervention in the following circumstances:

- when it is needed for entering into or the carrying out of a contract with you
- when the process is permitted by law
- when you have given explicit consent

In circumstances where we use special category data, for example, data about your health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership the company will ensure that one of the following applies to the processing:

- you have given your explicit consent to the processing; or
- the processing is necessary for reasons of substantial public interest

1.2 Data Breach Notification Policy

1.2.1 Aim

We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

1.2.2 Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. The following are examples of data breaches:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a data controller or data processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

1.2.3 Breach detection Measures

We have implemented the following measures to assist us in detecting a personal data breach:

- Employees shall be trained to recognise such breaches and regular staff awareness training will be provided.
- We shall understand the data access of **ALL** users within the organization and regularly monitor whether the data access is appropriate for a specific user.

1.2.4 Investigation Into Suspected Breach

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by the point of contact for data protection that will make a decision over whether the breach is required to be notified to the Data Protection Commission. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

1.2.5 When A Breach Will Be Notified To The Data Protection Commission

In accordance with the GDPR, we will undertake to notify the Data Protection Commission of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Data Protection Commission will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned
- the name and contact details of the point of contact for data protection where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

1.2.6 When A Breach Will Be Notified To The individual

In accordance with the GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

- a description of the nature of the breach
- the name and contact details of the point of contact for data protection where more information can be obtained
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

1.2.7 Record Of Breaches

HCT Learning records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

1.3 Subject Access Request Policy

1.3.1 Aim

You have a right, under the General Data Protection Regulation, to access the personal data we hold on you. To do so, you should make a subject access request, and this policy sets out how you should make a request and our actions upon receiving the request.

1.3.2 Definitions

"Personal data" is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including your name.

"Special categories of personal data" includes information relating to:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics

- biometrics (where used for ID purposes)
- health
- sex life or
- sexual orientation

1.3.3 Making A Request

Although subject access requests may be made verbally, we would advise that a request may be dealt with more efficiently and effectively if it is made in writing. If you wish to make a request, please use the Data Access Request Form which is located on the website or you can call the office.

Requests that are made directly by you should be accompanied by evidence of your identity. If this is not provided, we may contact you to ask that such evidence be forwarded before we comply with the request.

Requests made in relation to your data from a third party should be accompanied by evidence that the third party is able to act on your behalf. If this is not provided, we may contact the third party to ask that such evidence be forwarded before we comply with the request.

1.3.4 Timescales

Usually, we will comply with your request without delay and at the latest within one month. Where requests are complex or numerous, we may contact you to inform you that an extension of time is required. The maximum extension period is two months. All learner assessment material is destroyed six months after the certification period.

1.3.5 Fee

We will normally comply with your request at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may contact you requesting a fee. This fee must be paid in order for us to comply with the request. A fee of €15 will apply to requests for the return of assessment materials.

In addition, we may also charge a reasonable fee if you request further copies of the same information.

1.3.6 Information You Will Receive

When you make a subject access request, you will be informed of:

- whether or not your data is processed and the reasons for the processing of your data
- the categories of personal data concerning you
- where your data has been collected from if it was not collected from you
- anyone who your personal data has been disclosed to or will be disclosed to, including anyone outside of the EEA and the safeguards utilised to ensure data security
- how long your data is kept for (or how that period is decided)
- your rights in relation to data rectification, erasure, restriction of and objection to processing
- your right to complain to the Office of the Data Protection Commissioner if you are of the opinion that your rights have been infringed
- the reasoning behind any automated decisions taken about you

1.3.7 Circumstances In Which Your Request May Be Refused

We may refuse to deal with your subject access request if it is manifestly unfounded or excessive, or if it is repetitive. Where it is our decision to refuse your request, we will contact you without undue delay, and at the latest within one month of receipt, to inform you of this and to provide an explanation. You will be informed of your right to complain to the Office of the Data Protection Commissioner and to a judicial remedy.

We may also refuse to deal with your request, or part of it, because of the types of information requested. For example, information which is subject to legal privilege or relates to management planning is not required to be disclosed. Where this is the case, we will inform you that your request cannot be complied with and an explanation of the reason will be provided.

1.4 Data Retention Policy

All hardcopy information will be stored in a locked, and secure location in HCT Learning’s offices, and once information has been updated to MyHCT and/or is no longer required, it will be disposed of through an outsource document destruction service company. These procedures comply with all legislation requirements, ensuring that our client, employee, and learner information is kept confidential and secure at all times. Current policy is that this will be destroyed six months after the certification period.

1.5 Assessment Holding Policy

After certification, HCT will store the learners assessments in a secure location on site for a period of 6 months. Learners may wish to request their assessments to be returned to them and HCT are happy to oblige this request. Please note there is an administration and courier cost of €15 applied to this service. All assessments are securely destroyed six months after the certification date. In the case of plagiarism, assessments will not be returned to the learners.

1.5.1 Personal Data Stored Online

- Photo identification
    - This will be deleted six months after the certification period.
- Learners assessment
    - Photographic and video evidence is gathered as evidence of skills demonstrations for some programmes.
        - Photographic evidence is uploaded by the trainers onto MyHCT under the relevant programme.
        - Video evidence is submitted to the office on a USB stick or on the company camcorder. This is uploaded to the online shared files. This is then deleted from the camcorder and USB stick. All assessment material online will be deleted six months after the certification period.

1.5.2 Personal Data Not Stored Online

In addition to the online storage of HCT Learning's data, HCT Learning also require hardcopy documentation to be gathered. This documentation is generally a part of our programme recruitment, entry and accreditation requirements. Examples of this type of data include:

- All learner assessment related documentation
    - They contain information such as full name, address, date of birth, gender, contact details, education, and career history.
        - This information is shared with Lantra for certification purposes.
        - Videos and photographs may be viewed by a third party such as an External Authenticator for certification purposes.
- For trainer and staff recruitment:
    - Copies of certificates
    - CVs

- Next of kin details
- Heath Questions

1.6 Definitions Of Data Protection Act

Data: means automated and manual data

Automated data: means information that:

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, or is

b) recorded with the intention that it should be processed by means of such equipment.

Manual data: means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

What is personal data: "personal data" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Sensitive personal data: means personal data as to the following:

(a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject.

(b) whether the data subject is a member of a trade union.

(c) The physical or mental health or condition or sexual life of the data subject.

(d) The commission or alleged commission of any offence by the data subject.

(e) Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Controller: a data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

Data Processer: is a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of their employment.

Data subject: is an individual who is the subject of personal data.

Processing of or in relation to information or data: means performing any operation or set of operations on the information or data, whether or not by automatic means, including:

(a) Obtaining, recording or keeping the information or data.

(b) Collecting, organising, storing, altering or adapting the information or data.

(c) Retrieving, consulting or using the information or data.

(d) Disclosing the information or data by transmitting, disseminating or otherwise making it available.

(e) Aligning, combining, blocking, erasing or destroying the information or data, and cognate words shall be construed accordingly.

Relevant filing system: means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

1.7 A37 Data Access Request Form

HCT
Progressive, Innovative & Interactive Training

Controller: Hughes Consultancy & Training Ltd t/a HCT Learning
Unit 2 Purcellsinch Business Park
Dublin Rd
Kilkenny

Data Subject:

Name:
Address:
Phone Number:

We require proof of identity to ensure the request being made is legitimate. This is in accordance with Data Protection guidelines.

ID Provided:

Details of Request:

Applicant is seeking to: (Please tick as appropriate)

Access Personal Data	
Rectify Personal Data	
Erase personal Data	

Details you are requiring access to:

Details you are requiring to be rectified: