DH Associates Ltd

Data Protection Policy

01 August 2021

Data Protection Policy

Contents

1 Legislative Framework

1. Data Protection Act 2018 and supporting/complimentary legislation

2. General Data Protection Regulation (GDPR).
This piece of legislation came in to force on the 25th May 2018. 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.

For the purpose of this policy, 'The data protection legislation' means:

(a) the GDPR, The GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
(b) The applied GDPR,
(c) The Data Protection Act 2018 and regulations made under this Act, and
(d) Regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive.

2. Purpose

The Company is committed to all aspects of data protection and takes seriously its duties, and the duties of its Employees, under the Data Protection Act 2018 and GDPR. This policy sets out how the Company deals with personal data, including personnel files and data subject access requests, and Employees' obligations in relation to personal data.

The purpose of the Data Protection Policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the General Data Protection Regulations (2016) and Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default. This policy covers:

• Our data protection principles and commitment to common law and legislative compliance;

• Procedures for data protection by design and by default.

3. Scope

All Employees, irrespective of their role within the organisation, are held by the contents of this policy and are required to follow and uphold the values, principals and expected behaviours of the Company when carrying out their duties and responsibilities.

4. Policy Statement

We need to collect and use personal information about people in order to provide our services and carry out our business. These may include members of the public, current, past and prospective employees, clients, customers and suppliers. In addition, we may be required by law to collect and use information. It is the Company's policy that all personal information, whether in paper, electronic or any other format, must be handled in strict confidence and managed in accordance with DPA and associated legislation and guidance.

5. Roles and Responsibilities

5.1 The Board of CareTech Group

The board of CareTech Group is responsible for the governance of DH Associates.

5.2 The Senior Management Team CareTech

The Senior Management Team has responsibility for information governance. This involves providing high level support to ensure that DH Associates applies relevant information governance policies and controls, including compliance with the requirements of the Data Protection Act 2018.

5.3 The Data Protection Officer

The Data Protection Officer is responsible for:
• Acting as the first point of contact for all data protection issues
• Providing guidance and advice on data protection issues
• Renewing and amending data protection notifications to the ICO
• Coordinating, processing and responding to all subject access requests
• Overseeing all data sharing protocols and agreements
• Creating, maintaining and renewing training modules and toolkits as appropriate
• Providing data protection training and awareness raising
• Coordinating and investigating information breach procedures.

5.4 DH Associates Senior Leadership Team

DH Associates Senior Leadership Team are responsible for ensuring that this policy and any associated procedures governing the use of personal information are in place understood and followed by all staff within their service. In addition they must:

- Ensure that their staff has access and resources to receive data protection training appropriate to their role

- Report any suspected breaches of confidentiality or information loss to the Data Protection Officer and follow any subsequent procedures

- Identify any existing or emerging information risks relating to personal information and report to the Data Protection Officer

- Ensure that personal data required to answer a subject access request is provided timely to the Data Protection Officer

- Ensure that there are appropriate procedures and measures in place to protect personal data, particularly when that information (hardcopy and electronic) is removed from the Company's premises

- Undertake annual information self assessments to ensure ongoing compliance with this policy

- Consult the Senior Management Team and Data Protection Officer before entering into any information sharing protocol or agreement.

5.5 Employees

Employees have a responsibility for data protection and must:

• Read, understand and follow this policy and any associated procedures that relate to the use and handling of personal information in the course of their work

• Undertake data protection training and ensure they have a clear understanding of their responsibilities when using and handling personal information

• Identify and report any risks to personal information to their line manager and/or the Data Protection Officer

• Identify and report suspected breaches of confidentiality or compromised personal data to their line manager and/or the Data Protection Officer

• Identify and forward any subject access requests to the Data Protection Officer to ensure that requests can be processed in accordance with the statutory timescales

• Assist clients in understanding their information rights and the Company's responsibilities in relation to data protection.

6 Underpinning Policies and Procedures

This policy is underpinned by the following:
• Data Quality (Record Retention) Policy
• Email and Internet Useage Policy

• Business Continuity Policy & Plan.

7 Data Protection Principles

The Data Protection Act 2018 requires that six data protection principles be followed in the handling of personal data. These principles require that personal data must:

1. be fairly and lawfully processed and in a transparent manner; DH Associates will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. be processed for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes; DH Associates will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3. be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; DH Associates will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4. be accurate and kept up to date; DH Associates will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the DH Associates if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the DH Associates to ensure that any notification regarding the change is noted and acted on.

5. kept for no longer than is necessary. DH Associates undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means DH Associates will undertake a regular review of the information held and implement a weeding process. DH Associates will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6. handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage DH Associates recognises that Individuals have various rights under the legislation including a right to:

- be told the nature of the information DH Associates holds and any parties to whom this may be disclosed.

- prevent processing likely to cause damage or distress.

- prevent processing for purposes of direct marketing.

- be informed about the mechanics of any automated decision making process that will significantly affect them.

- not have significant decisions that will affect them taken solely by automated process.

- sue for compensation if they suffer damage by any contravention of the legislation.

- take action to rectify, block, erase or destroy inaccurate data.

- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

DH Associates will only process personal data in accordance with individuals' rights. All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. DH Associates will ensure that all personal data is accessible only to those who have a valid reason for using it.

DH Associates will have in place appropriate security measures e.g.

- ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):
- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- archiving personal data which are then kept securely (lockable cabinet).
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.

In addition, DH Associates will put in place appropriate measures for the deletion of personal data

- Manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work.
- Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

DH Associates will ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data DH Associates will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA. Therefore, DH Associates will always seek the consent of individuals before placing any personal data (including photographs) on its website. If DH Associates collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

The Data Protection Act applies only to information that constitutes 'personal data'. Information is 'personal data' if it:

• identifies a person, whether by itself, or together with other information in the Company's possession, or is likely to come into its possession; and

• is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

Consequently, automated and computerised personal information about Employees held by employers is covered by the Act. Personal information stored physically (for example, on paper) and held in any 'relevant filing system' is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.

A 'relevant filing system' means a well-structured manual system that amounts to more than a bundle of documents about each Employee filed in date order, i.e. a system to guide a searcher to where specific information about a named Employee can be located easily.

We will establish and maintain policies to ensure compliance with the Human Rights Act 1998, the common law duty of confidentiality and the GDPR and Data Protection Action 2018, and all other relevant legislation.

We will establish and maintain policies for the controlled and appropriate sharing of employer, learner user and staff information with other agencies, taking account all relevant legislation and citizen consent. Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in the Data Quality Policy. We ensure that it is as easy to withdraw as to give consent.
We will undertake annual audits of our compliance with legal requirements.
We acknowledge our accountability in ensuring that personal data shall be in accordance with the six principles as set above.

We uphold the 'Personal Data Rights' outlined in the GDPR;

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

In line with legislation we will have access to a Data Protection Officer (DPO) who will report to the highest management level of the parent company. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

7.1 The Use of Personal Information

The Data Protection Act applies to personal information that is 'processed'. This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it.

7.2 Sensitive Personal Data

Sensitive personal data' is information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership (within the meaning of the Trade Union and Labour Relations
- (Consolidation) Act 1992);
- physical or mental health or condition;
- sex life;
- commission or alleged commission of any criminal offence; and
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

8. Procedure

The Company will not retain sensitive personal data without the express consent of the Employee in question. The Company will process sensitive personal data, including sickness and injury records and references, in accordance with the six data protection principles. If the Company enters into discussions about a merger or acquisition with a third party, the Company will seek to protect Employees' data in accordance with the data protection principles.

8.1 Consequences of Non-Compliance

All Employees are under an obligation to ensure that they have regard to the six data protection principles (see above) when accessing, using or disposing of personal

information. Failure to observe the data protection principles within this policy may result in an Employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an Employee accesses another Employee's employment records without the requisite authority, the Company will treat this as gross misconduct and instigate its disciplinary procedures.

Such gross misconduct will also constitute a criminal offence.

8.2 Personnel Files

An Employee's personnel file is likely to contain information about his/her work history with the Company and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the Employee including address details and national insurance number. There may also be other information about the Employee located within the Company, for example in his/her line Manager's inbox or desktop; with payroll; or within documents stored in a relevant filing system.

The Company may collect relevant sensitive personal information from Employees for equal opportunities monitoring purposes. Where such information is collected, the Company will anonymise it unless the purpose to which the information is put requires the full use of the individual's personal information. If the information is to be used, the Company will inform Employees on any monitoring questionnaire of the use to which the data will be put, the individuals or posts within the Company who will have access to that information and the security measures that the Company will put in place to ensure that there is no unauthorised access to it.

The Company will ensure that personal information about an Employee, including information in personnel files, is securely retained. The Company will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

The Company provides training on data protection issues to all Employees who handle personal information in the course of their duties at work. The Company will continue to provide such Employees with refresher training on a regular basis. Such Employees are also required to have confidentiality clauses in their contracts of employment.

Where laptops are taken off site, Employees must follow the Company's relevant policies relating to the security of information and the use of computers for working at home/bringing their own device to work.

8.3 Data Subject Access Requests

The Company will inform each Employee of:
• the types of information that it keeps about him/her;

• the purpose for which it is used; and
• the types of Company that it may be passed to, unless this is self-evident (for example, it may be self-evident that an Employee's national insurance number is given to HM Revenue & Customs).

An Employee has the right to access information kept about him/her by the Company, including personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the Employee is the focus of the email and documents that are about the Employee.

The Company will respond to any data subject access request within 28 calendar days. The Company will allow the Employee access to hard copies of any personal information. However, if this involves a disproportionate effort on the part of the Company, the Employee shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by the Company. The Company may reserve its right to withhold the Employee's right to access data where any statutory exemptions apply.

8.4 Correction, Updating and Deletion of Data

The Company has a system in place that enables Employees to check their personal information on a regular basis so that they can correct, delete or update any data. If an Employee becomes aware that the Company holds any inaccurate, irrelevant or out-of-date information about him/her, he/she must notify the HR department immediately and provide any necessary corrections and/or updates to the information.

8.5 Data that is Likely to Cause Substantial Damage or Distress

If an Employee believes that the processing of personal information about him/her is causing, or is likely to cause, substantial and unwarranted damage or distress to him/her or another person, he/she may notify the Company in writing to request the Company to put a stop to the processing of that information.

Within 21 days of receiving the Employee's notice, the Company will reply to the Employee stating either:

• that it has complied with or intends to comply with the request; or
• the reasons why it regards the Employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

8.6 Monitoring

The Company may monitor Employees by various means including, but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, the Company will inform the Employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used.

The Employee will usually be entitled to be given any data that has been collected about him/her. The Company will not retain such data for any longer than is absolutely necessary.

In exceptional circumstances, the Company may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the Company by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means (for example, where an Employee is suspected of stealing property belonging to the Company). Covert monitoring will take place only with the approval of a Director.

8.7 Employees' Obligations Regarding Personal Information

If an Employee acquires any personal information in the course of his/her duties, he/she must ensure that:

- the information is accurate and up to date, insofar as it is practicable to do so;
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- the information is secure.
-

In particular, an Employee should ensure that he/she uses password-protected and encrypted software for the transmission and receipt of emails; sends fax transmissions to a direct fax where possible and with a secure cover sheet; and locks files in a secure cabinet.

Where information is disposed of, Employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an Employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an Employee acquires any personal information in error by whatever means, he/she shall inform the Company immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within the Company.

Where an Employee is required to disclose personal data to any other country, he/she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact the HR Department.

An Employee must not take any personal information away from the Company's premises save in circumstances where he/she has obtained the prior consent of the Company to do so. If an Employee is in any doubt about what he/she may or may not do with personal information, he/she should seek advice from the HR Department.

8.8 Taking Employment Records off Site

An Employee must not take employment records off site (whether in electronic or paper format) without prior authorization. Any Employee taking records off site must ensure that he/she does not leave his/her laptop, other device or any hard copies of employment records on the train, in the car or any other public place. He/she must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

8.9 Review of Procedures and Training

The Company will provide training to all Employees on data protection matters on induction and on a regular basis thereafter. If an Employee considers that he/she would benefit from refresher training, he/she should contact their Line Manager in the first instance. The Company will review and ensure compliance with this policy at regular intervals.

9. Guidance for Directors, Managers and Staff

This guidance has been developed to assist staff at all levels to uphold the policy principles contained within the policy document on data protection and confidentiality. This section highlights the duty of confidence owed to customers, employers, learners and staff by the Company and by each individual member of staff. It provides information on specific areas of responsibility, and it highlights the application of the Data Protection Act to manual as well as computer held records, and the resulting implications.

9.1 Implementing the Policy

The Company's policies on Data Protection and Confidentiality apply throughout all regions and departments, without exception. Responsibility for ensuring implementation of the policy within each region lies with the director, who may delegate that responsibility to an appropriate assistant/Manager. The Company will review and ensure compliance with this policy at regular intervals.

9.2 Staff Awareness

To secure staff awareness of their data protection and confidentiality responsibilities, all contracts of employment with the Company must contain a duty of confidentiality clause. In addition, all newly appointed staff must receive information about their responsibilities regarding the protection of personal information. Managers must ensure that all newly appointed staff attend and completes the staff induction programme, which includes advice on the protection of information. A copy of this policy should be readily available for reference in services.
The Data Protection and Confidentiality policies require that all information on customers, employers, learners and staff is treated in strict confidence and in compliance with legislative requirements and guidance provided in the Data Protection Act and associated legislation and guidance. The following information is provided to help all staff meet their responsibilities in respect of data protection.

It is important that staff are aware that the Company will take disciplinary action against any and all members of staff found to have breached confidentiality. Staff should also be aware that they risk personal prosecution for breaches of the DPA, especially where they have failed to take account of the requirements of this policy.

9.3 Records and Record Keeping

Personal information should be adequate, relevant and not excessive for the reason(s) for which it is collected or used. Personal information should be accurate and kept up to date. All records should be clear, relevant and concise, and indicate the identity of any persons who have made an entry in them. The use of abbreviations (where these are not standardised or agreed) and jargon should be avoided.

9.4 Passing Information to Next Of Kin

When staff join the company they complete a next of kin information to identify who should be contacted in an emergency. Consent to share basic information in an emergency is therefore agreed.

9.5 Photographic, Audio, and Video Recordings of Learners and Use of Data on Social Media

• In all cases, of photographic, audio and video recordings, consent is required and refusal to participate must be respected. Consent can be given verbally and recorded and dated in the learner notes. The completion of a consent form is recommended where recordings or images are likely to be published.

• Social media must never be used in a way that conflicts with or breaches any organisational policy. Personal confidentiality of employees or clients must be respected at all times.

• Social media should not be used to make defamatory or disparaging comments about any employee, learner, employer or any business partners of DH Associates

• Employees will be personally responsible and accountable for any images that breach confidentiality or contain sensitive information; are speculative or discriminatory or contain information that might identify a learner.

9.6 Use of Fax Machines

Due to increased risks to the confidentiality and security of personal information, fax machines must not be used to transmit personal identifiable data or other confidential information unless in exceptional circumstances and approved by the l Director.

9.7 Use of Email

Personal-identifiable information sent by email within Company must be done within the requirements of the Data Protection Act and individual staff members are responsible for ensuring the confidentiality of information they send by email. Information can be transferred across the Company email network in the knowledge that the system is secure and protected, however staff should still protect any file attachments that are sensitive or contain personal level information. In all cases, only the minimum information must be sent by email and great care must be taken to ensure the correct email address is used.

Personal information about learners or staff should not be emailed either to or from any staff member's personal computer or personal email account. No identifiable data may be stored on laptops or devices such as USB sticks, unless protected by encryption software.

Portable PCs containing identifiable information must be locked away when not in use and staff using portable PCs with this type of information must take all reasonable steps to guard against theft or loss and against unauthorised use.

9.8 Media Enquiries

All media enquiries must be directed to the Chief Operating Officer (COO).

9.9 Removal of Records from Company Premises by Staff

The removal of records from premises by staff, except in the following circumstances, is prohibited:
• When a learner is being transferred to another training provider
• When a member of staff is making a visit and must take a employer and /or learner notes along.
• When notes are needed for evidence in a court case and the attending member of staff cannot collect them on the day of the hearing.
• When other working practices require professional staff to take records home overnight (to be returned to premises as soon as possible).

9.10 Minimum Retention Periods

ESFA requires all funded apprenticeship learner records to be retained for 6 years, from contract year 2017.

All ESF funded learning including apprenticeships pre May 2017 must be retained until 31 December 2030.

All awarding body records must be retained for 3 years.

All personnel records must be retained for 6 years from the date the employee left the organisation.

.

9.11 Data Security and Continuity

• To prevent damage to our IT systems, all computing equipment must be authorised by the IT Department before being used with our existing systems. This includes desktop PCs, laptops, smart phones and printers.

• To prevent copyright infringements, security breaches, virus infections and other damage to DH Associates systems, all software must be authorised by the Finance/IT Department before being installed or used with our IT systems. This includes store-bought and downloaded programs, screen savers, logos, games, video and music files.

• All users have their own username and password.

• Usually passwords are eight alphanumeric.

Users are made aware that their system password is the equivalent of their signature and that they must not divulge their password to others, nor must they seek other user's passwords. If their password has become known by another, they must change it immediately.

• Symantec Enterprise software is the antivirus protection. This updates automatically from the manufacturer and every time a user logs on to the company network the computer gets updated with the latest antivirus definitions. Daily scans are in place. Every Cloud software is also used for filtering mail and web use.

• An enterprise version of Symantec and Cisco hardware and Software firewalls are in place and they are regularly managed and maintained by the IT team and the IT services provider who are contracted to manage this service.

• Services have access to a central company drive to store confidential information and records. This can be accessed from a different terminal in the event of a system breakdown or disaster situation.

• Disaster recovery of data/access to data is in place with the online backup provider.

The backups take place daily and are stored in a secure data centre. The IT team regularly perform tests and real time restores and these are only performed upon approval of a Director level for the respective department/person.