Data Protection Policy

Coventry & Warwickshire Chamber of Commerce Training

Training | Skills | Growth

Scope

C&W CHAMBER TRAINING is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998 and the General Data Protection Regulations 2018. **C&W CHAMBER TRAINING** processes information about its staff, learners, employers and other individuals it has dealings with for a range of administrative purposes (e.g. to recruit and pay staff, administer programmes of learning and comply with legal obligations of funding bodies and Government). In order to comply with the law, information about individuals must be collected and used fairly, stored safely and securely, retained for only so long as is necessary and not disclosed to any third party unlawfully.

All "processing" of personal data (includes collection, holding, retention, destruction and use of personal data) are governed by the Data Protection Act 1998 and the General Data Protection Regulations 2018. It applies to all personal data - whether it is held on a computer or similar automatic system or whether they are held as part of a manual file. Personal data is defined as information relating to an identifiable living individual and can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Under the Data Protection Act 1998, all organisations that process personal information are required to notify the Information Commissioner's Office. **C&W CHAMBER TRAINING's** Notification describes the various types of processing of personal information and defines the persons or bodies to which the information may be disclosed - the registration number is Z6925846.

The General Data Protection Regulations 2018 afford further protection of the privacy of personal data, including the right to erase personal data and withdraw consent.

It is an offence to process personal data except in strict accordance with the **eight principles of data protection** and the **rights of data subjects**. Further information on the Data Protection Act can be found at https://www.legislation.gov.uk/ukpga/1998/29/contents and the General Data Protection Regulations at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Failure to comply with the above could result in the prosecution not only of **C&W CHAMBER TRAINING** but also of the individual concerned.

Data subjects (that is persons about whom such data is held) may also sue for compensation for damage and any associated distress suffered as a result of:

- loss or unauthorised destruction of data
- unauthorised disclosure of, or access obtained to, data
- inaccurate data - i.e. data which is incorrect or misleading

It follows, therefore, that all staff who are concerned with, or have access to, such data have an obligation to ensure that they are processed according to the eight principles of data protection and the rights of data subjects.

This means, among other things, that staff must treat all data carefully and must not disclose personal data to unauthorised persons (this will often include parents and carers of learners).
C&W CHAMBER TRAINING does not authorise any employee or agent of **C&W CHAMBER TRAINING** to hold or process any personal data on its behalf. Users of personal data should consider the legal position before attempting to process personal data.

In cases of doubt or difficulty staff should in the first instance contact the Executive Director of **C&W CHAMBER TRAINING.**

REMEMBER - TREAT PERSONAL DATA WITH CARE
DON'T PASS ON PERSONAL INFORMATION TO UNAUTHORISED PERSONS

Eight Data Protection Principles

- Data should be processed fairly and lawfully
- Data should be obtained for one or more specified lawful purposes
- Data shall be adequate, relevant and not excessive
- Data shall be accurate and where necessary kept up to date
- Data is not kept longer than is necessary for its purpose
- Data shall be processed in accordance with subject rights under the Act
- Appropriate technical and organisational measures shall be taken against unauthorised/unlawful processing, loss, destruction, damage to personal data
- Data shall not be transferred outside EEA unless that country/territory ensures adequate level of protection for rights and freedoms of data subjects in relation to the processing of personal data

C&W CHAMBER TRAINING is committed to making sure that:

- All information is lawfully processed
- Information is only processed for limited purposes, for example for funding returns to Government bodies
- Information stored is adequate and relevant
- Information is accurate
- Information will not be kept longer than necessary
- Information held will be processed in line with the rights of the person to which it refers
- Information is stored securely and only accessed by approved, authorised individuals who have undergone Disclosure and Baring Service screening
- Information will not be transferred to countries that do not have suitable data protection laws
- Staff, learners and other clients are entitled to view any information about them by applying to the Executive Director

Data Security

C&W CHAMBER TRAINING's data security refers to the protective digital privacy measures that are applied to prevent unauthorised access to computers, databases and websites. This includes:

- Encryption of laptops
- No staff PC or workstation to be left unmanned without a password protected screen saver
- All staff PCs or workstations to be closed down and password protected out of working hours
- All staff to only use their own log-in to access PCs and other devices and not share their log-in details with others
- Daily back-up of data arrangements off-site in a secure location
- Application of anti-virus software across its IT network with regular updates

Staff passwords are changed every 8 weeks and meet complexity requirements, including:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)

All staff, upon obtaining employment, will receive information on data security and **C&W CHAMBER TRAINING**'s data privacy arrangements as a component of the induction process as well as interim update training.

Procedure for Data Breach

Whilst every care is taken to safeguard personal data from incidents (either accidentally or deliberately), compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative compliance and/or financial cost.

Data security breaches include confirmed or suspected incidents, an event or action which may compromise the confidentiality, integrity or availability of systems or data which may cause or potentially cause harm to **C&W CHAMBER TRAINING's** information assets and/or reputation.

An incident includes:

- Loss or theft of confidential or sensitive data or equipment on which the data is stored (laptop, USB stick, tablet, mobile phone or paper record)
- Equipment failure or loss
- System failure
- Unauthorised use of, access to, data or information systems
- Attempt to gain access to information or IT systems
- Unauthorised disclosure of sensitive/confidential data
- Hacking of systems
- Human error
- Disclosure of information by staff to deceiving organisations

Reporting Arrangements

Any individual member of staff who accesses, uses or manages **C&W CHAMBER TRAINING**'s information is responsible for reporting a data breach and information security incidents immediate to the Executive Director.

If the breach occurs outside of normal office hours, it must be reported as soon as is practicable.

The report must include full and accurate details of the incident, when the breach occurred (date/time), person reporting it, nature of the information, the number of individuals involved. An Incident Report Form should be completed as part of the reporting procedure (Appendix 1).

All staff should be aware that any breach of data security may result in disciplinary action in line with company policy.

The Executive Director will establish the severity of the breach and appoint an investigating officer as appropriate. The investigation will gather information, assess the extent of the incident, limit the damage the breach could cause, identify who needs to be notified and determine a course of action. An investigation will take place within 2 working days of the breach being discovered/reported.

The investigation will include an assessment of:

- Type of data involved
- Sensitivity of the data
- Protection arrangements of data
- Circumstances of the loss
- Data subjects affected by the breach
- Wider organisational consequences

Notification

The investigating officer will consult with relevant colleagues to determine whether the Information Commissioner's Office require notification. If so, this will be completed within 72 hours.

Every incident will be assessed on its own merits, case by case, considering:

- Whether the breach is such that an individual's rights under data protection legislation are affected
- Whether notification would prevent unauthorised or unlawful use of personal data
- Whether there are legal or contractual notification requirements

Individuals, whose personal data has been affected by an incident which has a high risk of adversely affecting an individual's rights, will be informed as soon as is practicable. Notification will include a description of how and when the breach occurred and the data involved, including what action has been taken to mitigate the risk.

A record will be kept of any personal data breach, regardless of whether it was deemed notifiable.

Evaluation

The senior management team will review the causes of the breach and effectiveness of action taken to identify whether changes are required to systems and processes. Existing controls will be assessed with regard to adequacy (staff awareness; system security).

Data Subject Rights

Individuals have the right to make ***subject access requests*** regarding the nature of information held about them and to know to whom it has been disclosed. This includes the right to:

- Prevent processing likely to cause damage or distress
- Prevent processing for purposes of direct marketing
- Be informed about mechanics of automated decision making process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by automated process
- Take action for compensation if they suffer damage by any contravention of legislation
- Take action to rectify, block, erase or destroy inaccurate data
- Take action to withdraw consent for collection and use of personal data
- Request the Commissioner to assess whether any provision of legislation has been contravened

Procedure for Subject Access Requests

Individuals wishing to access their personal information should submit a request in accordance with the following notes:

1. Make a request, in writing, to the Executive Director (see below for contact details).
2. The request should include details and provide documented evidence of who the individual is (e.g. driving licence, passport, birth certificate). It should also provide as much detail as possible regarding the information in question (e.g. where and by whom information is believed to be held, specific details of information required etc).
3. It is required to state WHY an individual wishes to access the information: the details required are merely those that will aid the efficient location and retrieval of information.
4. Once the Executive Director receives a subject access request, all efforts will be made to fully comply within a calendar month. In any event, you will receive all the information that has been located and can be released within that period along with an explanation for any information that cannot be provided at that time.
5. In accordance with the Data Protection Act 1998 and General Data Protection Regulations 2018, **C&W CHAMBER TRAINING** does not usually release information held about individuals without a legal obligation, legitimate interest or individual consent. Therefore if information held about you also contains information related to a third party, **C&W CHAMBER TRAINING** will make every effort to anonymise the information. If this is not possible, and **C&W CHAMBER TRAINING** has been unable to secure the relevant consent, **C&W CHAMBER TRAINING** may decide not to release the information.

All queries should be directed to **C&W CHAMBER TRAINING's** Executive Director in the first instance.

Name: Executive Director

Email: enquiries@cw-chambertraining.co.uk

Postal Address: C&W CHAMBER TRAINING
Commerce House
St Nicholas Street
Coventry CV1 4FD

Telephone: 024 7623 1122

Policy Review

C&W CHAMBER TRAINING's data protection policy will be updated as required to ensure compliance with relevant legislation and reviewed on an annual basis.

Coventry & Warwickshire Chamber of Commerce Training

Data Breach Report Form

Appendix 1

Any suspected or actual data breach must be promptly reported to the Executive Director at enquiries@cw-chambertraining.co.uk using this form.

Section 1: To be completed by the individual reporting the incident or appropriate Manager

Name of person reporting the incident:	
Date of incident discovery:	
Location of incident:	
Contact details of person reporting the incident (email; telephone):	
Brief description of the incident/details of the information loss:	
Number of data subjects affected (if known):	
Brief details of any action taken at the time of the discovery:	

Signature:		Date:	

Section 2: To be completed by the Executive Director

Received by:		Date:	
Forwarded for action to:		Date:	
Signature:		Date:	

Section 3: To be completed by the Investigating Officer

Received by:		Date:	
Signature:		Date:	

Section 4: To be completed by the Investigating Officer as part of the investigation

Name of Investigating Officer:		Date:	
Incident No:			
Details of the IT systems, equipment, devices, records involved in the security breach:			
Details of the information loss:			
Extent of information loss:			
Extent of loss on business operations, legal liabilities, reputational consequences:			
Number of data subjects:			
Implications (if any) on contractual security arrangements:			
Nature of the sensitivity of the data (including any special categories – ethnic origin, religious belief, gender, health, sexual orientation):			
Information that could be used to commit identity fraud (personal bank information, national identifiers including NI number, copies of passport, birth certificate):			
Information relating to vulnerable adults or children:			
Information relating to individuals, including work performance, remuneration, personal life that could cause distress to an individual if disclosed:			
Information relating to progress of students or discipline or sensitive information which could adversely affect individuals:			
Signature:		Date:	

Section 5: To be completed by the Investigating Officer as part of the outcome of the investigation

Name of Investigating Officer:		Date:	
Incident No:			
Extent of information loss:			
Reported to internal stakeholders (specify who):			
Action taken by responsible persons:			
Notification to ICO: Yes / No If Yes Details:			
Notification to Data Subjects: Yes / No If Yes Details:			
Notification to external stakeholders: Yes / No If Yes Details: