General Data Protection Regulation (GDPR) Policy

General Data Protection Regulation (GDPR) Policy

1.0 Policy Statement

1.1 The General Data Protection Regulation (GDPR) replaces the Data Protection Act 1998 (DPA) which came into force on the 1st March 2000 in the UK. It governs the processing of personal data and becomes legally enforceable in the UK on the 25th May 2018, although the legislation is already legally approved.

This evolution of data protection regulation law was introduced to extend the protection of 'personal data' and clearly defines regulations on who can decide how and why personal data is processed with clear obligations to ensure that appropriate procedures and processes are in place to enable good information management, as defined by a set of clear principles and rules.

For the purposes of the GDPR personal data is defined as *"any information relating to an identified or identifiable natural person*".

The key principles of the new GDPR are:

- **Lawfulness, fairness and transparency.**
- **Purpose limitation.**
- **Data minimisation.**
- **Accuracy.**
- **Storage limitation.**
- **Integrity and confidentiality.**

C-Learning holds personal data about its associates and customers and wider clients, suppliers and wider individual data for a variety of purposes necessary to conduct its business.

This policy sets out how we will protect personal data and ensure that everyone involved in the operation of C-Learning understands the rules and principles governing the use of personal data which they may access in undertaking their duties. It is a requirement of this policy that staff must ensure that the Data Protection Officer (DPO) is consulted before any significant new data processing activity is initiated to ensure compliance with the relevant regulations and legislation. For C-Learning the DPO will be the Executive Chairman.

This policy requires anyone conducting work with or for C-Learning to abide by the rules and regulations it outlines. Any failure to comply with the policy could result in disciplinary proceedings or legal action being taken.

Everyone at C-Learning is responsible for:

- Checking that any information provided to the C-Learning in connection with their duties is accurate and up to date.

- Informing C-Learning of any changes to information they have provided such as a change of address.

- C-Learning cannot be held accountable for any errors unless they have been informed of changes relating to the personal data in question.

2.0 Scope

2.1 The General Data Protection Regulation (GDPR) applies equally to digital and/or paper records held in any system from which any individual might reasonably be identified.

As with existing data protection legislation the GDPR can apply to personal data held visually in photographs or video clips (including CCTV) or as sound recordings. C-Learning does not collect a large amount of personal data adopting a minimum data approach in its business and has a responsibility to ensure full compliance with the letter and spirit of both current data protection legislation and the extended rights and responsibilities of the GDPR.

3.0 Key Principles

3.1 Awareness.

It is the responsibility of everyone at C-Learning to ensure adequate awareness of their responsibilities under the GDPR and wider data protection legislation.

3.2 Information Audit.

C-Learning will make a best effort to maintain the accuracy and currency of the data it holds, the source and location of the data and who is responsible for it.

3.3 Privacy Information

C-Learning will review its privacy notices and ensure that appropriate plans and processes are in place to comply with the letter and spirit of the GDPR.

C-Learning will make the legal basis for collection of data transparent, document data retention periods and inform people that they have a right to complain to the ICO (Information Commissioner's Office) if they perceive a problem with the processing of their data that warrants it.

All language relating to the GDPR used by C-Learning will be clear and easy to understand.

3.4 Individual Rights

C-Learning will ensure systems and processes are in place to support the relevant rights of individuals in regard to their personal data including the deletion of personal data where appropriate and how data will be made available electronically or in a commonly used format as required.

The GDPR protects the following specific data rights for individuals:

- The right to be informed.
- The right of access.
- The right of rectification.
- The right to be forgotten (erasure of data in specific circumstances).
- The right to restrict processing of data in specific circumstances.
- The right to data portability.
- The right to object to the use of personal data.
- The right not to be subject to automated data driven decision making processes such as analytics profiling and auto-completion of opt-in on forms or similar.

3.5 Subject Access Requests

In most cases C-Learning will not charge for any requests made.

C-Learning will have a total of one month to comply with a subject access request. Currently the law permits 40 days.

C-Learning can charge for any request that is considered to be unfounded or excessive in regards to resource implications.

If C-Learning refuses a request the Chief Data Protection Officer (Executive Chairman) must justify to the individual why the request has been refused and clarify that they have the right to complain to the supervisory authority to seek judicial remedy. This must be actioned quickly and within a maximum of one month.

3.6 Lawful Basis for Processing Data

For C-Learning the lawful basis for the processing of data in regard to the GDPR is ‘Legitimate Interest’. As C-Learning only obtains a minimum amount of data by default in order to respond to enquiries and to conduct normal business with its clients, internal risk assessments indicate a low level of likelihood of harm in regard to the individual impact of a potential data breach. A majority of data currently used by C-Learning is not of a personal nature but rather relates to the details of the ‘business’ of the client.

3.7 Consent

Consent to process personal data must be based on the following principles. The consent must be freely given, specific, informed and unambiguous.

Affirmative action must be taken to opt in to any data processing where relevant.

There is no requirement to re-work all existing consent processes but compliance with the GDPR must be achieved by C-Learning at all times.

3.8 Children

The GDPR for the first time provides special protection for the personal data of children.

The GDPR defines the age of a child in regard to consent for data processing as anyone under the age of 16. It is possible that for the UK this may be lowered to 13 but currently the

legislation states 16. For anyone below this age consent must be secured from a person with ‘parental responsibility’ for the purposes of data processing.

3.9 Data Breaches

C-Learning will ensure it has appropriate procedures in place to detect, report and investigate a personal data breach. The data breach process is provided as Appendix 1 to this policy.

C-Learning is only obligated to report a data breach to the ICO where it is likely to result in a risk to the rights and freedom of individuals, for example where it might lead to reputational damage, loss of confidentiality, discrimination or wider social or economic disadvantage.

If anyone at C-Learning becomes aware of a data breach they must inform the Data Protection Officer (Executive Chairman).

Should a data breach occur the Executive Chairman will undertake a full and immediate risk assessment in regard to reputational, financial and operational risk. Where the breach is notifiable to the ICO the Executive Chairman will be responsible for reporting the breach within the required timescales. The nature and scale of the breach will determine how an individual is contacted to advise that their data may have been compromised. A communication plan will be implemented, depending on the individual circumstances of a breach, which will include any PR arrangements required to minimise the impact on individuals and the organisation.

3.10 Data Protection by Design

C-Learning will adopt a privacy by default model when it comes to data handling and processing. Privacy by design is now a legal requirement of the GDPR under the term ‘data protection by design and by default’.

3.11 Executive Chairman

C-Learning has appointed a designated Data Protection Officer, the Executive Chairman.

It is a requirement of the GDPR that the Data Protection Officer has the knowledge, support and authority to conduct the role effectively.

It is the responsibility of the Data Protection Officer to:

- Keep the Board/senior team updated about data protection responsibilities, risks and issues.
- Review all data protection procedures and policies on a regular basis.
- Provide appropriate briefings and information, advice and guidance on data protection for all stakeholders and those included in this policy.
- Respond to questions on data protection from stakeholders.

- Respond to individuals such as clients and employees who wish to know which data is being held that relates to them at C-Learning.

- Check and approve with third parties that handle the company's data any contracts or agreement regarding data processing.

The Data Protection Officer has daily operational responsibility for the implementation of this policy.

4 General Requirements of the GDPR

4.1 Key sensitive/special category data covered by the GDPR relates to:

- **Race.**
- **Gender.**
- **Politics.**
- **Religion.**
- **Health.**
- **Trade Union membership.**
- **Criminal record data.**
- **Genetic and biometric data.**

4.2 The only people able to access data covered by this policy should only be those who require that access to conduct their work.

4.3 C-Learning must keep all data secure by taking sensible and appropriate precautions some of which are highlighted below:

- **Strong passwords must be used and never shared.**

- **Personal data must never be disclosed to anyone unauthorised to access it.**

- **Data should be regularly reviewed and updated if it is found to be out of date. If the data is no longer required for the purposes of the organisation, it should be disposed of safely.**

- **Stakeholders should request advice and guidance in regard to any data protection assistance from the Data Protection Officer (Executive Chairman).**

- **Where personal information is stored on paper it should be kept in a secure place that would reasonably prevent any unauthorised person from accessing it easily and in a location where others cannot see it.**

- **Paper printouts containing personal information must not be left in a location where any unauthorised person might be likely to see it, such as on a printer/photocopier.**

- **Paper printouts containing personal information should be shredded and disposed of securely when no longer required.**

- **Electronic data must be stored securely and reasonably protected from unauthorised access, accidental deletion or malicious cybercrime.**

- **Removable storage media should not be used as the organisation has secure cloud storage provided by Google which is fully GDPR compliant.**

- **Data that just requires storage should only be stored on Google Drive as a fully backed up and GDPR compliant storage solution. Local drives and servers must not be used for this purpose.**

- **All data should be backed up (either automatically through Google) or through appropriate disaster recovery mechanisms. Recovery procedures should be tested regularly.**

- **All servers and computing devices processing or containing personal data must be protected by approved security software and a firewall that would provide external scrutiny with assurance of full GDPR compliance.**

- **When working with personal data everyone at C-Learning must ensure that their computer screens are locked when left unattended.**

- **Personal data should not be shared via informal channels such as an email. An email is not a secure method of communication.**

- **Data that is being transferred outside of C-Learning should be encrypted.**

- **Data should be held in as few places as possible and necessary. C-Learning will avoid creating additional datasets where possible.**

- **C-Learning will take every opportunity to ensure that personal data is updated. For example by confirming a clients personal details over a call.**

- **C-Learning will ensure that data subjects can easily update the personal information held about them.**

- **Data should be updated as inaccuracies are discovered. This may include a client that can no longer be reached on the number stored for example and it should then be removed from the database.**

Appendix 1

C-Learning Data Breach Process