General Data Protection Regulation (GDPR) Policy and Procedures

Data Protection Policy Statement

Cornerstone Learning CIC takes data protection very seriously. As such, this policy outlines the measures that are put in place to ensure the protection of all personal and sensitive data about children we work with and their families and other individuals.

The ICO is the UK's data protection regulator. Cornerstone Learning CIC is registered with this regulator and is set to pay an annual fee.

This policy outlines a data protection by design culture within Cornerstone Learning CIC so that all collection, storage and processing of data, whether digital or on paper, is carried out lawfully in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.

● Password protecting reports using the child's DOB in the format ddmmyy when emailing.

● Using strong passwords on email and laptops.

● Never sharing passwords.

● Personal data should not be disclosed to unauthorised people, either within the company or externally.

● Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data storage These rules describe how and where data should be safely stored.

● When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

● These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

● When not required, the paper or files should be kept in a locked drawer or filing cabinet.

● Data printouts should be shredded and disposed of securely when no longer required.

● When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts

● Data should be protected by strong passwords that are changed regularly and never shared between employees.

● If data is stored on removable media (like a memory stick), these should be kept locked away securely when not being used.

Data should be backed up frequently. Those backups should be tested regularly.

All computers containing data should be protected by security software and a firewall.

Data use When working with personal data, screens of computers are always locked when left unattended.

Personal data must be passworded before being transferred electronically.

Personal data should never be transferred outside of the European Economic Area.

Data accuracy The law requires the organisation take reasonable steps to ensure data is kept accurate and up to date.

● It the responsibility of the consultant to take reasonable steps to ensure data is kept as accurate and up to date as possible.

● Data will be held in as few places as necessary.

● Data should be updated as inaccuracies are discovered. For instance, if a client can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests All individuals who are the subject of personal data held by Carina Greening are entitled to: • Ask what information the company holds about them and why. • Ask how to gain access to it. • Be informed how to keep it up to date. • Be informed how the company is meeting its data protection obligations. If an individual contacts the company requesting this information, this is called a subject access request.

● Subject access requests from individuals should be made by email, addressed to the data controller at cornerstone.learningcic@gmail.com

● The data controller can supply a standard request form, although individuals do not have to use this.

● The data controller will aim to provide the relevant data within 14 days.

● The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Cornerstone Learning CIC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Quality Assurance

Cornerstone Learning will ensure that systems are in place to monitor the implementation of and compliance with this policy and accompanying procedures. The directors will ensure action is taken to swiftly remedy any identified weaknesses within its procedures.

Policy Dates

This policy was written and takes effect February 2024

Paulina Malolepsza BSc
Director at Cornerstone Learning CIC