General Data Protection Policy and Procedure

How we collect, use and protect your personal data

CoreEd Limited

Version 2.0 | Review Date: 31/07/2026

1. Overview

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA.

2. What GDPR Covers

GDPR defines personal data as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In other words, any information that can identify an individual, whether online or in person, is governed by the protections afforded by GDPR.

There are obligations placed on organisations who collect and use personal data for their business purposes (data controller) and any organisations they share that personal data with (data processors) in order to achieve their business objective — for example, providing goods or services, online marketing, building websites etc. The data controller has a primary obligation to ensure that they obtain the relevant legal basis in order for the data processor to fulfil processing activities on its behalf. In other words, the data controller may need to obtain the consent of its customers to process their personal data through third parties.

3. CoreEd's Approach to GDPR Compliance

As part of our compliance with GDPR standards, CoreEd Limited has completed a data audit to identify the types of personal data that we interact with in the provision of our services to clients. The approach outlined below details the controls and mechanisms CoreEd Limited has in place to meet these standards.

Administrative Data

Administrative Data covers our learners' and employers' personal data, such as names, personal and/or business email addresses, telephone numbers and any other personal data provided during the course of our ongoing relationship. This personal data is one for which CoreEd Limited is the data controller, as we determine the appropriate measures and controls in order to protect this personal data from unauthorised use, disclosure and access.

CoreEd Limited therefore has the primary responsibility for the protection of this personal data. CoreEd Limited takes the protection of this data extremely seriously and ensures that personal data is stored securely and protected in line with GDPR.

Client Data

The nature and scope of personal data which our learners and employers provide to us will depend on the nature of the client's business and the CoreEd Limited services procured. In other words, this is the client's data and that of their clients, and may vary depending on their business or the service required.

The client, as a data controller, and CoreEd Limited, as a data processor, have joint responsibilities under GDPR for ensuring that there are appropriate technical and organisational measures in place for the protection of this personal data. The appropriate measures will vary depending on the scope of personal data involved in the services. Nevertheless, CoreEd Limited undertakes a baseline standard for these controls for the protection of personal data.

Technical Measures — Business Processes

In order to carry out business-as-usual activities and general delivery of services, CoreEd Limited uses various platforms and applications to run and manage its internal processes. This may include the sharing of documentation, communications, emails and file-sharing systems, either internally or between CoreEd Limited and its clients. CoreEd Limited scrutinises the security and integrity of products and applications before incorporating them into its business processes. Applications include, but are not limited to, Microsoft 365, Microsoft Teams and SharePoint.

4. Learner Rights

Learners have the following rights in relation to the personal data we hold about them:

Right to be Informed You have the right to know what data we hold about you and how we use it.	**Right of Access** You can request a copy of the personal data we hold about you.
Right to Rectification You can ask us to correct any inaccuracies in the data we hold.	**Right to Erasure** You can request deletion of your personal data in certain circumstances.
Right to Restriction You can ask us to temporarily stop processing your personal data.	**Right to Data Portability** You can ask for your data in a format that allows you to transfer it to another party.
Right to Object You can object to the inclusion of any of your personal information.	**Automated Decision-Making** You have the right to regulate any automated decision-making and profiling of your personal data.

5. Data Security

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to:

- Store files of written information of a confidential nature securely so that they are only accessed by people who have a need and a right to access them.
- Ensure that screen locks are implemented on all PCs, laptops and other devices when unattended.
- Ensure no files or written information of a confidential nature are left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

> Personal data relating to learners must not be kept or transported on laptops, USB sticks or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by encryption. Laptops and USB drives must not be left where they can be stolen.

Failure to follow CoreEd Limited's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

6. Data Breaches

All data breaches will be recorded on our Data Breach Register. Where legally required, CoreEd Limited will report a breach to the Information Commissioner's Office (ICO) within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to the breach.

7. Data Protection Officer

Our appointed Data Protection Officer in respect of our data protection activities is:

Data Protection Officer
Airam Neesa
Airam@CoreEd.co.uk
07912 342367

8. Monitoring, Review and Evaluation

The implementation of this policy is reviewed and evaluated through the self-assessment process. A copy of this policy is accessible to all staff via the SharePoint folder and the CoreEd website.

CoreEd Limited is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Date of review: 31/07/2025 Next review: 31/07/2026