

General Data Protection Policy and Procedure

How we collect, use and protect personal data

CoreEd Limited

Version 3.0 | Review Date: 31/07/2027

1. Purpose and Scope

This policy sets out how CoreEd Limited collects, uses, stores and protects personal data, and what every member of staff must do when handling it. It is the internal operating policy. The version written for learners, employers and the public is the GDPR and Privacy Policy (P-007).

It applies to all staff, associates and contractors who handle personal data on CoreEd's behalf, and to all personal data CoreEd holds, whether about learners, applicants, employers, staff or anyone else.

2. The Law That Applies

The EU GDPR no longer applies directly in the United Kingdom

Since the end of the transition period, data protection in the UK is governed by the UK General Data Protection Regulation, the Data Protection Act 2018 and the Data (Use and Access) Act 2025. Keeping Children Safe in Education 2026 refers to these collectively as the data protection laws. References to the EU GDPR in older documents should be read as references to the UK regime.

- UK General Data Protection Regulation
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications Regulations 2003
- Keeping Children Safe in Education 2026 and Working Together to Safeguard Children 2026, in respect of safeguarding information sharing

3. Definitions

Personal data	Any information relating to an identified or identifiable living individual, whether directly or indirectly, including by reference to a name, identification number, location data or online identifier.
Special category data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation. It requires an additional condition for processing.
Data controller	The organisation that determines the purposes and means of processing. CoreEd is the data controller for the personal data it collects about learners, applicants, employers and staff.

Data processor	An organisation that processes personal data on the instructions of a controller. CoreEd's third-party support providers act as processors under a data processing agreement.
Processing	Anything done with personal data, including collecting, recording, storing, using, sharing, altering and deleting it.
ROPA	Record of Processing Activities, required by Article 30 of the UK GDPR.
DPIA	Data Protection Impact Assessment, required before processing that is likely to result in a high risk to individuals.

4. CoreEd's Role

CoreEd is the data controller for the personal data it holds about learners, applicants, employers, staff and visitors. That means CoreEd determines why and how the data is used, and holds primary responsibility for protecting it.

Where CoreEd engages a third party to process personal data on its behalf, for example a learner support provider or a systems supplier, that organisation acts as a data processor. CoreEd enters into a written data processing agreement with every processor, requires appropriate technical and organisational measures, and does not permit sub-processing without prior written consent.

Where an employer of an apprentice holds and uses data about their own employee, that employer is a controller in its own right. The relationship is set out in the Learner Data Sharing Agreement (P-019).

5. Lawful Basis and Data Minimisation

Personal data is processed only where CoreEd has a documented lawful basis. The bases CoreEd relies on are contract, legal obligation, legitimate interests, and consent where required. Special category data, including health, disability and safeguarding information, additionally relies on a condition in Schedule 1 to the Data Protection Act 2018, most commonly the safeguarding of children and individuals at risk condition, or explicit consent.

Staff collect only the personal data needed for the purpose, keep it accurate and up to date, and do not use it for a new purpose without checking that a lawful basis covers it. The lawful basis for each processing activity is recorded in the Record of Processing Activities.

6. Staff Responsibilities

Every member of staff who handles personal data must:

- store confidential written information securely so that only those with a need and a right can access it
- lock screens on all devices when unattended
- leave no confidential information where it can be read by unauthorised people
- use CoreEd systems and approved applications only, and not personal accounts or personal storage
- encrypt or password protect computerised data, whether on a local drive or a network drive
- share personal data only with those who need it, and only through secure channels
- report a suspected data breach immediately, in line with Section 9
- complete data protection training at induction and annually

Removable media and devices

Personal data relating to learners must not be kept or transported on laptops, memory sticks or similar devices without prior authorisation. Where it is, it must be encrypted. Devices must not be left where they can be stolen. Where removable media is used, it must itself be kept in a locked cabinet, drawer or safe.

Failure to follow these rules may be dealt with under the Disciplinary Policy and Procedure (P-027). Sanctions include dismissal, with or without notice, depending on the severity.

7. Technical and Organisational Measures

- CoreEd scrutinises the security and integrity of any product or application before adopting it into business processes. Applications in use include Microsoft 365, Microsoft Teams, SharePoint, Aptom and MyConcern
- access is role based and granted on a need to know basis, with safeguarding and pastoral records restricted to named roles
- multi-factor authentication is applied to CoreEd systems
- data is encrypted in transit, and network drives are backed up regularly
- audit trails are maintained for significant data sharing activity
- cyber security measures are applied in line with the Cyber security standards for schools and colleges, as set out in the Online Safety and Remote Learning Policy (P-036)

Personal data is not transferred outside the United Kingdom without appropriate safeguards under Chapter V of the UK GDPR.

8. Individual Rights

Right to be informed	To know what data CoreEd holds, why, and how it is used. Met through the GDPR and Privacy Policy (P-007) and the privacy notice issued at enrolment.
Right of access	To request a copy of the personal data CoreEd holds about them, together with information about its use.
Right to rectification	To have inaccurate or incomplete data corrected without undue delay.
Right to erasure	To request deletion, in certain circumstances and where no retention obligation applies.
Right to restriction	To request that processing is restricted while a challenge is resolved.
Right to data portability	To receive data they provided in a structured, commonly used, machine-readable format, and to have it transmitted to another controller.
Right to object	To object to processing based on legitimate interests, and to object to direct marketing at any time.
Rights on automated decisions	Not to be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects.

Responding to a request

Any request from an individual to exercise a right is passed to the Data Protection Lead on the day it is received, however it arrives and whether or not it uses the correct words. A request does not have to be in writing or use any particular form.

CoreEd responds within one calendar month, extendable by up to two further months for complex or numerous requests, in which case the individual is told within the first month. Requests are logged, and no fee is charged unless a request is manifestly unfounded or excessive.

9. Data Breaches

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It includes an email sent to the wrong recipient, a lost device and unauthorised access to a system.

Step	Action	Timescale
1. Report	Any member of staff who becomes aware of an actual or suspected breach reports it to the Data Protection Lead immediately. Do not attempt to resolve it alone and do not delete anything.	Immediately
2. Contain	The Data Protection Lead takes steps to contain the breach and recover the data where possible.	Same day
3. Assess	The Data Protection Lead assesses the risk to the rights and freedoms of the individuals affected and records the assessment.	Within 24 hours
4. Report to the ICO	Where the breach is likely to result in a risk, it is reported to the Information Commissioner's Office. Where it is not, the reasons are recorded.	Within 72 hours of becoming aware
5. Inform individuals	Where the breach is likely to result in a high risk, the individuals affected are told in clear and plain language.	Without undue delay
6. Record and learn	All breaches, reportable or not, are recorded on the Data Breach Register with the actions taken and lessons learned.	On conclusion

10. Records, Assessments and Retention

CoreEd maintains a Record of Processing Activities under Article 30, describing what personal data is held, why, the lawful basis, who it is shared with and how long it is kept. It is reviewed at least annually.

A Data Protection Impact Assessment is completed before any new processing that is likely to result in a high risk to individuals, including the adoption of a new system holding learner data, and before any significant change to existing processing.

Personal data is retained only for as long as necessary, in line with the Document Retention and Secure Storage Policy (P-020), and is disposed of securely at the end of the retention period.

11. Safeguarding and Information Sharing

Data protection is never a reason to withhold safeguarding information

The data protection laws do not prevent the sharing of information for the purposes of keeping learners safe. Fears about sharing information must not be allowed to stand in the way of safeguarding a learner. The Data Protection Act 2018 provides a processing condition for the safeguarding of children and

individuals at risk, which permits sharing without consent where there is good reason. Where a member of staff is in any doubt, they speak to the Senior DSL rather than withhold information. The Safeguarding Policy (P-013) governs.

12. Data Protection Lead

CoreEd's appointed lead for data protection is:

Airam Neesa, Director and CEO

Airam@CoreEd.co.uk | 07912 342367

The Data Protection Lead maintains the Record of Processing Activities and the Data Breach Register, oversees subject access requests, advises on Data Protection Impact Assessments, and is the point of contact for the Information Commissioner's Office.

Statutory Data Protection Officer

CoreEd is not a public authority and does not carry out large-scale systematic monitoring, so it is not required to appoint a statutory Data Protection Officer. Where an organisation does appoint one, the UK GDPR requires that the postholder does not determine the purposes and means of processing, which would prevent the Director and CEO from holding the role. CoreEd therefore designates a Data Protection Lead rather than a statutory Data Protection Officer, and keeps that position under review as the organisation grows.

13. Training

All staff complete data protection training at induction and annually. Training covers what personal data is, the lawful bases, the rules at Section 6, how to recognise and report a breach, how to recognise a subject access request, and the relationship between data protection and safeguarding. Completion is recorded and available for inspection.

14. Monitoring, Review and Evaluation

The Data Protection Lead monitors the operation of this policy, including breach volumes and causes, subject access request volumes and response times against the statutory deadline, training completion, and the currency of the Record of Processing Activities and processing agreements. Findings feed into the self-assessment process.

This policy is reviewed annually, or earlier where the law or CoreEd's processing changes. A copy is available to all staff via SharePoint and is published on the CoreEd website.

15. Associated Documentation

- Complaints Procedure (P-004)
- GDPR and Privacy Policy (P-007)
- Safeguarding Policy (P-013)
- Learner Data Sharing Agreement (P-019)

- Document Retention and Secure Storage Policy (P-020)
- Business Continuity Policy (P-025)
- Disciplinary Policy and Procedure (P-027)
- Online Safety and Remote Learning Policy (P-036)
- Record of Processing Activities, Data Breach Register and Data Processing Agreements
- Learner Privacy Notice, issued at enrolment

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.

Policy owner: Director and CEO

Date of review: 31/07/2026 **Next review:** 31/07/2027