Data Protection & GDPR Policy

Policy Approval						
Approval Required:	**Yes**	☒	**No**	☐	**Annual Review Required:**	Yes ☒ No ☐
Approval Panel:	Darren Powell					
Created By:	**Name**		**Signature**		**Date**	
	Darren Powell				01/09/2024	
Reviewed:	Darren Powell				01/08/2025 — No Changes	
Next Review Date:	August 2026					
Policy Writer/s:	Darren Powell					

STATEMENT

During the course of our activities, Cinders Training will process personal data (which may be held on paper, electronically, or otherwise) about our staff, learners and other stakeholders. We recognise the need to treat all personal data in an appropriate, lawful and transparent manner, in accordance with the Data Protection Act 2018 (DPA 2018) — the UK implementation of the UK General Data Protection Regulation (UK GDPR).

The purpose of this policy is to set out how Cinders Training collects, uses, stores and protects personal data, and to inform all relevant persons of their rights. This policy does not form part of any employee's contract of employment and may be amended at any time.

Cinders Training is registered with the Information Commissioner's Office (ICO), the UK's independent authority for information rights. Our ICO registration is maintained and renewed annually.

SCOPE

This policy applies to all employees, associates, learners, employers and other stakeholders whose personal data is processed by Cinders Training. It covers all personal data regardless of format — paper, electronic, audio or visual.

DATA PROTECTION LEAD

The designated Data Protection Lead for Cinders Training is the Head of Education & Quality. All data protection queries, Subject Access Requests, and data breach reports should be directed to: info@cinderstraining.co.uk

DATA PROTECTION PRINCIPLES

All personal data processed by Cinders Training must be:

- Processed lawfully, fairly and transparently

- Collected for specified, explicit and legitimate purposes, and not further processed incompatibly with those purposes
- Adequate, relevant and limited to what is necessary ('data minimisation')
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary ('storage limitation')
- Processed securely — protected against unlawful or unauthorised processing, accidental loss, destruction or damage

LAWFUL BASIS FOR PROCESSING

Cinders Training will only process personal data where there is a valid lawful basis under UK GDPR, including:

- Contractual necessity — to deliver training, assessment and qualification services
- Legal obligation — to comply with employment law, health and safety legislation, ESFA requirements, and awarding organisation requirements including Highfield Qualifications
- Legitimate interests — for quality assurance, business improvement and stakeholder communication
- Consent — where explicit consent has been obtained and recorded

For special category data (including health, ethnicity, criminal convictions), an additional condition under UK GDPR Article 9 or Schedule 1 DPA 2018 will be met, typically explicit consent or a legal/employment obligation.

HOW WE USE PERSONAL DATA

Staff Data

- Administering employment contracts, payroll and benefits
- Managing performance, absence and sickness
- Monitoring compliance with equal opportunities legislation
- CPD records and qualification tracking

Learner / Apprentice Data

- Registration with awarding organisations — including Highfield Qualifications via Highfield Central
- Delivery and assessment of qualifications and training programmes
- Submission of achievement data to awarding organisations and funding bodies
- Quality assurance monitoring and improvement
- Compliance with ESFA and funding body requirements

DATA RETENTION

Category of Data	Minimum Retention Period
Learner registration and qualification records	3 years minimum (Highfield requirement); longer if required by funding body
Assessment decisions and IQA records	3 years minimum after EQS review
Staff employment records	6 years after end of employment
Complaints and appeals records	5 years
Payroll and financial records	6 years

YOUR RIGHTS UNDER UK GDPR

- Right of access (Subject Access Request) — free of charge, responded to within one calendar month

- Right to rectification — request correction of inaccurate data
- Right to erasure — request deletion, subject to legal and contractual obligations
- Right to restriction of processing
- Right to data portability
- Right to object to processing based on legitimate interests or for direct marketing
- Rights relating to automated decision-making

SUBJECT ACCESS REQUESTS

Subject Access Requests must be submitted in writing to the Data Protection Lead. Responses will be provided free of charge within one calendar month of receipt. Proof of identity may be requested before releasing personal data.

DATA BREACH PROCEDURE

All suspected or actual data breaches must be reported to the Data Protection Lead immediately. Cinders Training will assess severity within 24 hours and, where the breach is likely to result in risk to individuals' rights and freedoms, report to the ICO within 72 hours. All breaches will be recorded regardless of whether reportable.

DATA SECURITY

- Password-protected systems with unique user logins changed regularly
- Encrypted storage of sensitive data where technically feasible
- Secure physical storage for paper records with restricted access
- Regular backups to Microsoft Office 365 server
- Staff training on data protection responsibilities
- Access to personal data limited to those who need it for their role

THIRD PARTY DATA SHARING

Personal data will only be shared with third parties where: the individual has consented; we are legally required to do so; it is necessary to deliver our services (e.g. sharing with Highfield Qualifications for registration and certification); or a written Data Processing Agreement (DPA) is in place ensuring equivalent protection.

BREACHES OF THIS POLICY

Any breach of this policy will be taken seriously and may result in disciplinary action. Concerns should be raised with the Data Protection Lead or, where the Lead is involved, with the Managing Director.

POLICY REVIEW

This policy will be reviewed annually or sooner following any significant data breach or change in legislation. All staff will be notified of material updates.

This policy should be read alongside: Business Continuity Policy, Quality Assurance Policy, Malpractice and Maladministration Policy, and the IT Security Procedure.