Data Protection (GDPR) Policy

Version: 1.2

Approved by: Directors

Date Approved: 22/09/2026

Next Review: 21/08/2027

Policy Owner: Directors

DOCUMENT CONTROL

Document Title	**Data Protection (GDPR) Policy**
Organisation	Reach Education and Employment
Author	Christopher Murray
Approved By	Directors
Date Approved	22/09/2026
Review Date	21/08/2027
Version	1.2
Next Review	Annual

Key Data Protection & Supervisory Authority Contacts

Role / Authority	Contact Name / Detail	Contact Information
Designated Data Protection Officer (DPO) / Lead	Christopher Murray	07583695771 / chris@reach-education.org
Deputy Safeguarding & Privacy Lead	Jade Wilson	07772303522
Executive Director	Andrew Mallin	07740606684
Information Commissioner's Office (ICO)	UK Supervisory Authority	0303 123 1113 / www.ico.org.uk
NCFE Quality Assurance & Assessment Integrity	Centre Support & Compliance	0191 239 8000 / service@ncfe.org.uk

1. Policy Statement

Reach Education and Employment (REACH) is committed to protecting the personal data, privacy, and fundamental rights of learners, staff, directors, parents/carers, partner employers, and stakeholders. This policy sets out our operational procedures for collecting, processing, securing, sharing, retaining, and disposing of personal data in strict compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Data protection is integral to safeguarding, learner trust, and effective governance. This policy supports the mandatory delivery, quality assurance, and assessment security standards required to maintain approved NCFE Centre Status, ensuring that learner data and raw assessment portfolios remain secure and auditable at all times.

2. Scope

This policy applies across all Reach Education and Employment operations, covering all personal data processed in electronic, paper, photographic, video, and audio formats. It governs all learners (aged 16–25 and vulnerable adults/adults at risk), employees, sessional tutors, job coaches, directors, supply staff, volunteers, contractors, and

visiting assessors. It applies to data processed on organizational premises, remote/home environments, and cloud infrastructure.

Crucially, this scope encompasses all NCFE candidate registration logs, candidate identification records, live assessment test papers, portfolio tracking matrices, internally assessed marks, Access Arrangements logs, and internal quality assurance (IQA) audit trails.

3. Statutory Framework & FOIA Clarification

This policy is grounded in and complies with statutory legislation and awarding body regulations:

- UK General Data Protection Regulation (UK GDPR) & Data Protection Act 2018
- Freedom of Information Act 2000 (Clarification: As a Community Interest Company, REACH is not a designated public authority under Schedule 1 FOIA; however, REACH fully complies with statutory information disclosure duties where delivering services under contract with public bodies and local authorities, while handling all individual personal data requests strictly under UK GDPR Subject Access Rights)
- Section 16LA of the Children Act 2004 (Statutory Information Sharing Duty via Children's Wellbeing and Schools Act 2026)
- Keeping Children Safe in Education (KCSIE 2026) & Working Together to Safeguard Children 2023
- Human Rights Act 1998 (Article 8: Right to Respect for Private and Family Life)
- NCFE General Regulations, Centre Agreement Guidelines & Qualification Approval Criteria
- Joint Council for Qualifications (JCQ) General Regulations for Approved Centres

4. Key Definitions

- **Personal Data:** Any information relating to an identified or identifiable living individual (e.g. name, ID number, address, date of birth, attendance logs, ULN, examination marks).
- **Special Category Data:** Highly sensitive data requiring enhanced technical and legal safeguards under Article 9 UK GDPR, including racial or ethnic origin, religious beliefs, physical or mental health details, disability/SEND diagnostic data, biometric/genetic data, or sex life/sexual orientation.
- **Processing:** Any operation or set of operations performed on personal data, whether or not by automated means, including collection, recording, structuring, storage, retrieval, consultation, sharing, or erasure.
- **Data Controller:** The natural or legal person who determines the purposes and means of processing personal data. Reach Education and Employment is the Data Controller.

- **Adverse Effect (Awarding Body):** Any unexpected operational event, data loss, security compromise, or test material leak that threatens the integrity of assessment tasks, breaches confidential exam scripts, or threatens to invalidate a learner's raw qualification evidence.

5. Data Protection Principles (Article 5 UK GDPR)

Reach Education and Employment ensures that all personal data is processed strictly in accordance with the six core principles:

- Lawfulness, Fairness, and Transparency: Data is processed legally, fairly, and with clear privacy notices provided to data subjects.
- Purpose Limitation: Data is collected for specified, explicit, and legitimate educational/training purposes and not further processed in a manner incompatible with those aims.
- Data Minimisation: Processing is limited strictly to what is adequate, relevant, and necessary.
- Accuracy: Reasonable steps are taken to ensure personal data is accurate, complete, and kept up to date.
- Storage Limitation: Data is retained in identifiable form only for as long as necessary, complying with statutory retention schedules.
- Integrity and Confidentiality: Processed with appropriate technical and organizational security against unauthorized access, loss, or destruction.
- Accountability: The organization maintains verifiable documentation demonstrating active compliance, auditable for NCFE External Quality Assurers (EQAs) and the ICO.

6. Lawful Basis for Processing (Articles 6 & 9 UK GDPR)

REACH ensures that every data processing activity relies upon an identified lawful basis under Article 6 UK GDPR:

- Contractual Necessity: Necessary to deliver educational programmes, register candidates with NCFE, process certifications, and manage employee contracts.
- Legal Obligation: Necessary to comply with statutory duties, including funding returns to ESFA/DfE, safeguarding reports under KCSIE, and RIDDOR notifications to HSE.
- Public Task / Statutory Duty: Exercised in the public interest to deliver further education, vocational skills, and supported employment.
- Vital Interests: Processing necessary to protect an individual’s life or emergency medical welfare.
- Legitimate Interests: Exercised where organizational operational needs do not override the fundamental rights and freedoms of the individual.

- Explicit Consent: Relied upon for non-essential activities, including promotional photography, public case studies, or optional survey communications.

Special Category Data (Article 9): Processed under Article 9(2)(b) (employment and social protection law), Article 9(2)(h) (health and social care provision), Article 9(2)(g) (substantial public interest / safeguarding vulnerable individuals under Schedule 1 Data Protection Act 2018), or explicit consent.

7. Roles & Governance Responsibilities

Role / Lead	Data Protection & Assessment Governance Responsibilities
Board of Directors	Maintain ultimate governance; ensure adequate resourcing for data security and encrypted infrastructure; review policy and privacy notices annually.
Data Protection Officer (DPO) - Christopher Murray	Monitor compliance with UK GDPR; act as primary liaison with the ICO; advise on Data Protection Impact Assessments (DPIAs); investigate security breaches and lead Subject Access Requests.
Examinations Officer & Lead Assessors	Ensure accurate, timely entry of candidate registrations on NCFE portals; maintain absolute physical and digital security over unsealed test papers, controlled assessment briefs, and IQA records.
All Staff, Tutors & Job Coaches	Handle learner data with strict confidentiality; enforce password security; report data incidents immediately; complete mandatory annual data protection training.

8. Data Subject Rights & Subject Access Requests (SARs)

Data subjects possess clear statutory rights under UK GDPR: the right to be informed, right of access, right to rectification, right to erasure ('right to be forgotten'), right to restrict processing, right to data portability, and right to object to processing.

STATUTORY SUBJECT ACCESS REQUEST (SAR) PROTOCOL:
Operational SAR Procedure & Statutory Timescales:

• Submission: Data subjects may submit a Subject Access Request (SAR) verbally or in writing to Christopher Murray (DPO).
• Turnaround SLA: In compliance with Article 12 UK GDPR, REACH must respond to SARs within ONE CALENDAR MONTH of receipt (free of charge).
• Extensions: For highly complex or multiple requests, the response window may be extended by up to two additional months, provided the applicant is notified within the initial month with full rationale.
• Verification & Third Parties: Identity must be verified before releasing records. Third-party data must be redacted unless consent is obtained or disclosure is reasonable.
• Examination Exemption: Under Schedule 2 Data Protection Act 2018, exam scripts written by candidates are exempt from SAR disclosure. However, candidate marks, assessor feedback, and grading sheets must be provided once results are published.

9. Data Security and Assessment Integrity

Technical and organizational security measures enforce strict confidentiality across physical and cloud environments:

- Role-based access controls; mandatory multi-factor authentication (MFA); complex password requirements; full-disk encryption on all portable laptops; and automated screen-locking after inactivity.
- Live NCFE Examination Materials: Secure physical storage in a double-locked, fire-rated cabinet within an access-controlled room. Digital controlled assessments stored within permission-restricted cloud folders.
- Strict Prohibition: Staff are strictly prohibited from removing unmoderated learner evidence, raw assessment portfolios, or secure test keys from physical or organizational cloud environments without formal written DPO/Director authorization.

10. Data Sharing & Statutory Safeguarding Information Sharing

Personal data is shared only where there is an identified lawful basis, verified Data Processing Agreements (DPAs) are in place, and secure transmission protocols (encrypted email, password-protected portals) are enforced.

- Awarding Body Data: Candidate data, registration matrices, moderation samples, and certification claims are transmitted to NCFE via secure awarding body portals.
- Section 16LA Children Act 2004 (Statutory Information Sharing Duty): Under the Children's Wellbeing and Schools Act 2026, UK GDPR and the common law duty of confidentiality DO NOT prevent sharing information with statutory safeguarding partners (Police, NYSCP Social Care) where necessary to protect a child or vulnerable adult. Consent is not required where seeking it would elevate risk or cause delay.

11. Third-Party Data Processors & International Transfers

- **Processor Due Diligence:** Due Diligence: All third-party software vendors, cloud platforms, e-portfolio systems, and IT contractors acting as Data Processors must execute a legally binding Data Processing Agreement (DPA) under Article 28 UK GDPR.
- **Transfer Safeguards:** International Data Transfers: REACH restricts personal data storage to the UK or European Economic Area (EEA). Personal data will not be transferred outside the UK unless: (1) The destination country has an adequacy regulation issued by the UK Government; or (2) Appropriate safeguards are in place, such as the UK International Data Transfer Agreement (IDTA) or approved standard contractual clauses.

12. Data Retention & Secure Disposal

Personal data is retained in accordance with statutory, contractual, and regulatory schedules before permanent secure disposal:

Category of Record	Statutory / Awarding Body Retention Period	Disposal Protocol
NCFE Candidate Records & Portfolios	Minimum 3 years following final certification (mandatory NCFE Centre criteria)	Secure digital shredding / physical confidential destruction
Accident & First Aid Logs	3 years from the date of the last entry	Secure cross-cut shredding
HSE RIDDOR F2508 Incident Files	Minimum 6 years from the date of the incident	Confidential archive destruction
Safeguarding Child / Adult Case Files	Until the individual reaches age 25 (or 6 years post-departure for adults)	Secure archive review and authorized disposal
Staff Personnel & HR Files	6 years following termination of employment	Secure digital file wipe

13. Personal Data Breaches, ICO Reporting & Adverse Effects

A personal data breach involves the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. Staff must report any suspected breach immediately to Christopher Murray (DPO).

MANDATORY BREACH REPORTING SLAs:

Statutory Breach Escalation Pathways:

1. ICO Notification (Article 33 UK GDPR): If a breach is likely to result in a risk to the rights and freedoms of individuals, the DPO must notify the Information Commissioner's Office (ICO) within 72 HOURS of becoming aware. (Breaches unlikely to result in a risk are logged internally but not reported).
2. Data Subject Notification (Article 34 UK GDPR): Where a breach is likely to result in a HIGH RISK to individuals' rights and freedoms, the affected individuals must be notified without undue delay.
3. NCFE Adverse Effect Notification: If a breach involves unsubmitted examination papers, learner portfolios, or grading matrices, the Examinations Officer must immediately notify the NCFE Quality Assurance Team to protect qualification integrity.

14. Data Protection Impact Assessment (DPIA) Process

Under Article 35 UK GDPR, a formal DPIA must be conducted prior to introducing any new technology, system, or processing activity likely to result in a high risk to individuals. At REACH, a mandatory DPIA is executed prior to deploying: new online e-portfolio systems; remote proctoring/digital exam software; AI generative educational tools; or biometric/surveillance platforms.

15. Training, Governance & Policy Review

All employees complete mandatory UK GDPR and data protection training during Day 1 induction, supplemented by annual refreshers. Examination and quality verification personnel receive dedicated briefing sessions regarding awarding body secure data management. This policy is reviewed annually by the Board of Directors or immediately following statutory revisions.

REACH EDUCATION AND EMPLOYMENT

APPENDIX: NCFE 3-YEAR RETENTION AUDIT LOG SHEET

Mandatory Awarding Body Record Management | NCFE Centre Criteria

This log must be maintained accurately by the Examinations Officer and Internal Quality Assurers (IQAs). All records corresponding to registered NCFE cohorts must be retained securely for a minimum of 3 years post-certification before authorized disposal.

Cohort / ID	NCFE Title & Code	Evidence Type	Cert Date	Retention Expiry	Disposal Sign-off
NCFE-L2-EQD-2026	Level 2 Equality & Diversity (601/3145/7)	Portfolios / Grading	15/07/2026	15/07/2029	[Space for Sign]
NCFE-L3-BUS-2026	Level 3 Business Admin (601/3965/1)	IQA Sample Sheets	01/08/2026	01/08/2029	[Space for Sign]
NCFE-FS-ENG-2026	Functional Skills English L1/L2	External Exam Scripts	10/08/2026	10/08/2029	[Space for Sign]
NCFE-FS-MAT-2026	Functional Skills Maths L1/L2	Exam Result Portfolios	10/08/2026	10/08/2029	[Space for Sign]