Data Protection and GDPR Policy

Document Reference:	HTC-POL-OPS-002
Policy Owner:	Chief Operating Officer
Data Protection Lead:	Chief Operating Officer
Approved By:	Group Chief Executive Officer
Version:	2.0
Effective Date:	January 2026
Review Date:	January 2027

Version Control

Version	Date	Author	Changes
1.0	07/08/2024	Sophie Gilmore	Initial policy creation
1.1	26/08/2025	Patsy Crocker	Updated job titles
2.0	Jan 2026	Sophie Gilmore	Major revision: enhanced lawful bases, expanded data subject rights, detailed breach procedures, training provider-specific guidance, retention schedules

1. Purpose

Hybrid Training Centre (HTC) is committed to protecting the rights and privacy of all individuals whose personal data we process. This policy sets out our approach to data protection and compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

As a training provider, HTC processes significant amounts of personal data relating to learners, apprentices, employers, and staff. We recognise our responsibility to handle this data lawfully, fairly, and transparently, and to maintain the trust of all our stakeholders.

2. Scope

This policy applies to:

- All personal data processed by HTC, whether electronic or paper-based
- All HTC employees, contractors, and volunteers who process personal data
- All locations where HTC operates, including training centres and remote working
- Personal data of learners, apprentices, staff, employers, and other stakeholders

The policy covers data processing activities including collection, storage, use, sharing, and disposal of personal data.

3. Legal Framework

HTC's data protection obligations arise from:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003 (PECR)
- ESFA funding rules and data collection requirements
- Awarding organisation data sharing requirements

HTC is registered with the Information Commissioner's Office (ICO) as a data controller.

4. Key Definitions

Personal data: Any information relating to an identified or identifiable living individual. This includes names, addresses, email addresses, photographs, IP addresses, and any other information that could identify someone.

Special category data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation. Subject to additional protections.

Processing: Any operation performed on personal data, including collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, combination, restriction, erasure, or destruction.

Data controller: The organisation that determines the purposes and means of processing personal data. HTC is the data controller for the personal data it processes.

Data processor: An organisation that processes personal data on behalf of a data controller (e.g., cloud service providers, payroll providers).

Data subject: The individual whose personal data is being processed.

Data Protection Lead: The person responsible for overseeing data protection compliance at HTC (Chief Operating Officer).

5. Data Protection Principles

HTC adheres to the seven data protection principles set out in Article 5 of the UK GDPR:

5.1 Lawfulness, Fairness, and Transparency

Personal data must be processed lawfully, fairly, and in a transparent manner. Individuals must be informed about how their data will be used through clear privacy notices.

5.2 Purpose Limitation

Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

5.3 Data Minimisation

Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.

5.4 Accuracy

Personal data must be accurate and, where necessary, kept up to date. Inaccurate data must be corrected or erased without delay.

5.5 Storage Limitation

Personal data must be kept in identifiable form for no longer than necessary for the purposes for which it is processed.

5.6 Integrity and Confidentiality (Security)

Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

5.7 Accountability

The data controller must be able to demonstrate compliance with the above principles.

6. Lawful Bases for Processing

HTC only processes personal data where we have a lawful basis to do so. The lawful bases we rely on include:

Lawful Basis	Examples at HTC
Contract	Processing staff payroll; delivering training to enrolled learners
Legal obligation	ESFA data returns (ILR); tax and national insurance; safeguarding reporting
Legitimate interests	Marketing to employers; fraud prevention; business development
Consent	Marketing communications to learners; photographs for promotional use
Vital interests	Emergency contact in medical emergencies
Public task	Delivery of publicly-funded apprenticeships and training

For special category data, HTC must identify both a lawful basis and an additional condition for processing (e.g., explicit consent, employment law obligations, vital interests, or substantial public interest).

7. Data Subject Rights

Individuals have the following rights under data protection law. HTC respects and facilitates these rights:

7.1 Right to be Informed

Individuals have the right to know how their data is being used. HTC provides privacy notices at the point of data collection.

7.2 Right of Access (Subject Access Request)

Individuals can request a copy of the personal data HTC holds about them. Requests must be responded to within one month. There is no fee for standard requests.

7.3 Right to Rectification

Individuals can request correction of inaccurate or incomplete personal data.

7.4 Right to Erasure (Right to be Forgotten)

In certain circumstances, individuals can request deletion of their personal data. This right is not absolute and is subject to legal and regulatory retention requirements.

7.5 Right to Restrict Processing

Individuals can request that HTC restricts processing of their data in certain circumstances.

7.6 Right to Data Portability

Individuals can request their data in a machine-readable format for transfer to another organisation (where processing is based on consent or contract and is automated).

7.7 Right to Object

Individuals can object to processing based on legitimate interests or for direct marketing purposes.

7.8 Rights Related to Automated Decision-Making

Individuals have rights regarding automated decisions that have legal or significant effects on them.

Requests to exercise any of these rights should be made in writing to the Data Protection Lead at dataprotection@hybridtec.co.uk.

8. Responsibilities

8.1 Data Protection Lead (COO)

- Overall responsibility for data protection compliance
- Maintaining the data processing register
- Handling data subject requests and complaints
- Managing data breach responses
- Liaising with the ICO where required
- Ensuring staff training is delivered

8.2 All Staff

- Processing personal data only in accordance with this policy
- Keeping personal data secure
- Reporting suspected data breaches immediately
- Completing required data protection training
- Only accessing personal data necessary for their role

9. Data Security

HTC implements appropriate technical and organisational measures to protect personal data:

9.1 Technical Measures

- Password protection and access controls on all systems
- Encryption of data in transit and at rest where appropriate
- Regular software updates and security patches
- Antivirus and firewall protection

- Secure backup procedures
- Secure disposal of IT equipment

9.2 Organisational Measures

- Role-based access controls (staff only access data necessary for their role)
- Clear desk and clear screen policies
- Secure storage of paper records in locked cabinets
- Staff training on data protection
- Confidentiality clauses in employment contracts
- Due diligence on data processors

10. Data Breach Management

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

10.1 Reporting Breaches

All staff must report suspected data breaches immediately to the Data Protection Lead. Examples of breaches include:

- Loss or theft of devices containing personal data
- Sending personal data to the wrong recipient
- Unauthorised access to personal data
- Cyber attacks or ransomware
- Accidental deletion of data

10.2 Breach Response

On becoming aware of a breach, HTC will:

- Contain the breach and assess the risk
- Notify the ICO within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms
- Notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms
- Document the breach, its effects, and remedial actions taken
- Review and improve controls to prevent recurrence

11. Data Sharing

HTC shares personal data with third parties where necessary and lawful. Key data sharing includes:

- ESFA – Individualised Learner Record (ILR) data for funded learners
- Awarding organisations – learner data for registration and certification
- Employers – apprentice progress and attendance information
- End-Point Assessment Organisations – apprentice data for EPA
- Ofsted – learner data during inspections
- Service providers – IT support, payroll, etc. under data processing agreements

Data sharing with third parties is governed by data sharing agreements or data processing agreements as appropriate.

12. International Transfers

Personal data must not be transferred outside the UK unless adequate protections are in place. Where HTC uses cloud services or other processors that may process data internationally, we ensure that appropriate safeguards exist (adequacy decisions, Standard Contractual Clauses, or other approved mechanisms).

13. Data Retention

Personal data is retained only for as long as necessary. Key retention periods include:

Data Type	Retention Period
Learner records (funded programmes)	6 years from programme end (ESFA requirement)
Apprenticeship evidence	6 years from programme end
Assessment records	3 years (or as required by awarding organisation)
Staff employment records	6 years from end of employment
Recruitment records (unsuccessful)	12 months from decision
Safeguarding records	Until learner's 25th birthday (or longer if concerns)
CCTV footage	30 days unless required for investigation
Financial records	6 years (legal requirement)

Data is securely disposed of at the end of the retention period (shredding for paper, secure deletion for electronic data).

14. Training

All staff receive data protection training:

- Induction training for all new staff
- Annual refresher training for all staff
- Enhanced training for staff with significant data processing responsibilities

Learners are informed of their data protection rights during induction.

15. Related Documents

- Privacy Notice (Learners)
- Privacy Notice (Staff)
- Privacy Notice (Website)
- IT Acceptable Use Policy
- Information Security Policy
- Data Retention Schedule
- Data Breach Response Procedure
- Subject Access Request Procedure

16. Monitoring and Review

This policy is monitored through:

- Annual review of data processing activities
- Analysis of data subject requests and complaints
- Review of any data breaches and near-misses
- Staff training completion rates
- Internal audits of data handling practices

The policy is reviewed annually by the Data Protection Lead or sooner if required by changes to legislation or guidance.

Policy Approval

Signature: Date:

Sophie Gilmore
Group Chief Executive Officer