Data Protection (GDPR) Policy

Date created	14th September 2022
Owner	Mark Williams
Data Protection Officer (DPO)	Mark Williams
Version No	V2.3
Date last reviewed	20th October 2025
Date next review	19th October 2026

1. Introduction

This document sets out the obligations of iMeta Training ("the Company") regarding data protection and the rights of individuals with whom it works, in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This Policy establishes procedures to ensure that personal data is processed lawfully, fairly, and transparently. All employees, contractors, agents, consultants, and partners working on behalf of the Company must comply with these requirements.

The Company recognises that the lawful and responsible handling of personal data is vital to its reputation, contractual compliance, and relationships with learners, staff, and external partners.

2. The Data Protection Principles

Under the UK GDPR, all personal data must be:

1. Processed lawfully, fairly, and transparently.
2. Collected for specified, explicit, and legitimate purposes.
3. Adequate, relevant, and limited to what is necessary.
4. Accurate and kept up to date.
5. Retained only for as long as necessary.
6. Processed in a manner that ensures appropriate security.
7. Not transferred outside the UK or EEA unless adequate safeguards are in place.

3. Rights of Data Subjects

Data subjects have the following rights under the UK GDPR:

- The right to be informed about data collection and use.
- The right of access to their personal data.
- The right to rectification of inaccurate or incomplete data.
- The right to erasure ('right to be forgotten').
- The right to restrict or object to processing.
- The right to data portability.
- The right to lodge a complaint with the ICO.

4. Personal Data

Personal data refers to any information relating to an identifiable individual. This includes, but is not limited to:

- Names, addresses, and dates of birth
- National Insurance numbers and identification documents
- DBS checks and proof of right to work
- Contact details and employment history
- Bank account details and financial information
- Qualifications, certificates, and learner records

Sensitive personal data (special category data) includes information regarding racial or ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual orientation, and criminal records.

5. Processing Personal Data

All personal data is collected and processed for legitimate business, educational, or regulatory purposes. Data may be shared internally only with those who require access for specific tasks. The Company ensures that:

- Data is collected fairly and lawfully.
- Data subjects are informed of the purpose and use of their data.
- Personal data is accurate, up to date, and securely stored.
- Data is deleted or anonymised when no longer required.
- Transfers outside the UK/EEA are subject to appropriate safeguards.

6. Data Protection Procedures

- All emails containing personal data must be encrypted.
- Data stored electronically must be password-protected and encrypted.
- Hard copies must be kept in locked storage when not in use.
- Temporary or duplicate files must be securely deleted once no longer needed.

7. Technical and Organisational Security Measures

iMeta Training employs a range of security technologies and practices to protect the confidentiality, integrity, and availability of all personal data.

- **BitLocker Full-Disk Encryption:** All company laptops, external hard drives and USB memory sticks use BitLocker to encrypt data at the drive level. This prevents unauthorised access in the event of device theft or loss. Encryption keys are securely stored and managed by the IT Administrator.
- **Desktop Workstations:** At present, fixed workstations are not encrypted. These devices are kept in secure, access-controlled environments and are not used to store personal data locally. The Company is reviewing plans to extend BitLocker encryption to fixed workstations in the next review cycle to enhance compliance with UK GDPR Article 32.
- **Data in Transit Encryption:** All emails containing personal data are encrypted using TLS protocols.
- **Sophos Endpoint Protection:** Sophos provides real-time protection against viruses, malware, ransomware, and zero-day exploits. The system automatically isolates infected devices and prevents the spread of malicious code.
- **Sophos Phishing Protection:** Sophos includes advanced anti-phishing and email threat detection capabilities, scanning all inbound and outbound email traffic. Suspicious attachments and URLs are automatically quarantined, and users receive simulated phishing alerts to reinforce awareness.
- **Web Filtering and Application Control:** Sophos enforces web filtering to block known malicious domains and restricts unauthorised software installation.
- **Security Patch Management:** Software and operating systems are regularly updated to address known vulnerabilities.
- **Access Control:** Multi-factor authentication (MFA) is enforced across all cloud systems, and user privileges are restricted to the minimum required for each role.

8. Data Breach Management

iMeta Training maintains a structured procedure for identifying, reporting, and responding to data breaches:

- All staff must immediately report suspected breaches to the Data Protection Officer (DPO).
- The DPO will investigate, assess risks, and document findings.
- Where required, the DPO will notify the Information Commissioner's Office (ICO) within 72 hours.
- If the breach poses a high risk to individuals, affected data subjects will be informed promptly.
- A breach register is maintained for monitoring and continual improvement.

9. Organisational Measures

- The Company has appointed a Data Protection Officer (DPO) responsible for data protection compliance and oversight.
- All staff handling personal data receive mandatory data protection and cybersecurity training.
- Data protection compliance is reviewed annually.
- All third-party suppliers handling personal data must provide GDPR-compliant assurances and contracts.
- Failure to comply with this policy may result in disciplinary or contractual action.

10. Access by Data Subjects (DSARs)

Data subjects may request access to their personal data by submitting a Data Subject Access Request (DSAR) in writing to the DPO.
The Company shall:

- Acknowledge all DSARs promptly.
- Provide the requested information within one calendar month of receipt.
- Verify the requester's identity before disclosure.

11. Notification to the ICO

As a data controller, iMeta Training is registered with the ICO and renews its registration annually.

The DPO is responsible for maintaining the registration and notifying the ICO of any changes within 28 days.

12. Data Retention and Disposal

Personal data shall be retained only for as long as necessary to fulfil its intended purpose and meet legal or contractual obligations.

Data will be disposed of securely using a registered disposal company, with certificates of destruction retained. A separate Data Retention and Disposal Schedule defines specific retention periods.

13. Accountability and Documentation

To demonstrate compliance, iMeta Training maintains:

- Records of Processing Activities (ROPAs)
- Data Protection Impact Assessments (DPIAs) for high-risk processing
- Annual data protection audits
- Training and compliance logs

The Company reviews this policy annually or following significant legislative, operational, or technological changes.

14. Lawful Basis for Processing

Under Article 6 of the UK GDPR, iMeta Training identifies the lawful basis for processing personal data depending on the purpose and category of data involved:

- **Learner Data:** Processed under contractual obligation to deliver training and assess progress.
- **Employee Data:** Processed under legal obligation and contractual requirement for employment administration.
- **Partner and Supplier Data:** Processed under contractual obligation for business engagement.
- **Marketing and Alumni Data:** Processed under consent or legitimate interest, as appropriate.
- **Safeguarding Data:** Processed under legal obligation and in the public interest to ensure the welfare of learners.

The Company maintains a record of lawful bases for all processing activities within its Records of Processing Activities (ROPA).

15. Children and Vulnerable Learners

Where iMeta Training processes data relating to learners under 18 years old or vulnerable adults, additional safeguarding and parental consent procedures apply. The Company ensures compliance with Article 8 of the UK GDPR and relevant ESFA and Ofsted safeguarding standards. Personal data of minors is handled with heightened confidentiality and restricted access controls.

16. Data Sharing and Third-Party Processors

iMeta Training may engage third-party processors for functions such as data storage, payroll, or IT support.

All processors are vetted for GDPR compliance and are bound by Data Processing Agreements (DPAs) consistent with Article 28 of the UK GDPR.

Data sharing with external bodies (e.g. funding agencies, awarding organisations, or employers) is limited to what is necessary and performed under secure and lawful conditions.

17. Privacy Notices

iMeta Training maintains clear Privacy Notices for learners, staff, and partners that describe how personal data is collected, used, stored, and shared.

These notices are made available at the point of data collection and comply with Articles 13 and 14 of the UK GDPR.

The Privacy Notices outline data retention periods, rights of individuals, and how to contact the Data Protection Officer.

18. Security Review and Testing

All encryption configurations, BitLocker deployment, and Sophos protection systems are tested and validated during annual IT security reviews.

Penetration testing and phishing simulations are conducted periodically to assess resilience against evolving cyber threats.

The Company maintains documentation of all security reviews, encryption audits, and incident response exercises as part of its continuous improvement programme.

19. Data Protection Impact Assessments (DPIAs)

DPIAs are conducted whenever new technologies, systems, or processes are introduced that may present a high risk to individuals' privacy or rights.
This includes new learner management systems, data analytics platforms, or external data sharing arrangements.

The DPO oversees the completion and review of DPIAs to ensure mitigation of any identified risks.

20. Staff Training and Awareness

All staff, contractors, and associates receive mandatory induction training on data protection and cybersecurity.

Annual refresher training is provided to ensure continued awareness of responsibilities under UK GDPR.

Training completion and compliance records are maintained by the DPO.

21. Data Retention and Disposal Policy

iMeta Training ensures that personal data is retained only for as long as necessary for the purposes for which it was collected, in accordance with the UK GDPR's data minimisation and storage limitation principles.

Retention Principles

- Personal data shall be kept only as long as required to fulfil legal, contractual, or operational purposes.
- Retention periods are defined in a **Data Retention Schedule**, covering staff, learner, and partner data.
- Retention periods are reviewed annually by the Data Protection Officer (DPO).

Retention Period Examples

Data Type	Retention Period	Justification
Learner records	6 years after completion	ESFA funding and audit requirements
Employee HR files	6 years after termination	Employment law and reference requirements
Financial records	7 years	HMRC compliance
CCTV recordings	30 days	Security and safeguarding

Data Type	Retention Period	Justification
DBS and ID verification	Until recruitment checks completed	Legal requirement

Secure Disposal

- All paper records are shredded or disposed of through a **certified data disposal company**.
- All electronic data is permanently deleted using secure overwrite methods.
- Certificates of destruction are retained for all disposals.
- Tieva Backup and Restore ensures any deleted data is permanently purged at end of retention.

22. Information Security Policy

iMeta Training commits to maintaining the confidentiality, integrity, and availability of all information assets through robust technical and organisational controls.

Objectives

- Protect information from unauthorised access, loss, misuse, or alteration.
- Ensure compliance with UK GDPR, DPA 2018, and ISO 27001 principles.
- Support business continuity through secure backup and recovery.

Key Controls

- **Access Control:** Role-based access and MFA for all systems.
- **Device Security:** All laptops encrypted with BitLocker; desktops kept in secure areas.
- **Network Security:** Firewalls, VPNs, and network segmentation are implemented.
- **Threat Protection:** Sophos provides real-time malware, phishing, and ransomware defence.
- **Patch Management:** Updates are applied promptly to all systems.
- **Incident Management:** Any suspected breach or security incident is reported to the DPO immediately.
- **Monitoring and Review:** Logs, backups, and security alerts are reviewed regularly.

Business Continuity

- Tieva Backup and Restore ensures daily backups, encrypted both in transit and at rest.
- Disaster recovery testing is carried out at least annually.

Responsibilities

- The DPO oversees compliance and risk assessment.
- All staff are responsible for following this policy and completing annual security training.

23. Acceptable Use and Password Policy

Purpose
This policy defines acceptable use of company IT systems and data to prevent unauthorised access, disclosure, or misuse.

Acceptable Use Rules

- Company IT systems are provided for legitimate work purposes only.
- Users must not share accounts or passwords.
- Downloading unauthorised software or visiting unsafe websites is prohibited.
- Personal data must never be stored on unapproved devices or removable media.
- Email use must comply with professional and legal standards; phishing awareness is mandatory.

Password Policy

- Minimum password length: **12 characters**.
- Passwords must contain uppercase, lowercase, number, and special character.
- Passwords must be changed every 90 days.
- MFA is required for cloud systems and administrative accounts that have it as a requirement.
- Passwords must never be shared or written down.
- Compromised passwords must be reported immediately to IT.

Monitoring
System use may be monitored for compliance with security and data protection standards. Breaches may result in disciplinary or legal action.

24. Related Documents

- Privacy Notice (Learners, Staff, Partners)
- Incident Response Plan

This integrated framework ensures iMeta Training's compliance with UK GDPR, DPA 2018, and the ESFA funding rules.

All staff must read, understand, and confirm acceptance of these policies annually.