GDPR POLICY

Date of authorisation:	August 2024
Author / Reviewer responsible:	DONNA REYNOLDS
Reviewed by:	MICHELLE HOWDLE
Last amended:	August 2024
Date of next review:	August 2025

1. Introduction

Alpha Training is committed to complying with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy outlines how Alpha Training collects, processes, stores, and protects personal data to ensure compliance with legal requirements and uphold the rights of individuals.

2. Purpose

The purpose of this policy is to:

- Ensure compliance with GDPR and data protection laws.
- Protect the rights and privacy of individuals whose data Alpha Training processes.
- Provide clear guidance on data protection responsibilities for staff and learners.
- Outline procedures for handling personal data, including collection, processing, storage, and sharing.

3. Scope

This policy applies to:

- All employees, volunteers, and contractors of Alpha Training.
- All personal data processed by Alpha Training, including data relating to learners, staff, visitors, and any other individuals.

4. Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person (data subject).
- **Data Subject**: An individual whose personal data is processed by Alpha Training.
- **Processing**: Any operation performed on personal data, including collection, storage, use, and deletion.
- **Data Controller**: Alpha Training, which determines the purposes and means of processing personal data.
- **Data Processor**: Any third party that processes personal data on behalf of Alpha Training.
- **Consent**: Freely given, specific, informed, and unambiguous indication of the data subject's wishes to process their personal data.

5. Data Protection Principles

Alpha Training adheres to the following GDPR principles:

1. **Lawfulness, Fairness, and Transparency**: Personal data will be processed lawfully, fairly, and in a transparent manner.
2. **Purpose Limitation**: Personal data will be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. **Data Minimisation**: Personal data will be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.
4. **Accuracy**: Personal data will be accurate and, where necessary, kept up to date.
5. **Storage Limitation**: Personal data will be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data is processed.
6. **Integrity and Confidentiality**: Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage, using appropriate technical or organisational measures.
7. **Accountability**: Alpha Training will be responsible for and able to demonstrate compliance with these principles.

6. Lawful Basis for Processing

Alpha Training processes personal data under the following lawful bases:

- **Consent**: The data subject has given clear consent for processing their personal data for specific purposes.
- **Contractual Necessity**: Processing is necessary for the performance of a contract with the data subject or to take steps at their request before entering into a contract.
- **Legal Obligation**: Processing is necessary for compliance with a legal obligation to which Alpha Training is subject.
- **Vital Interests**: Processing is necessary to protect the vital interests of the data subject or another person.
- **Public Task**: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- **Legitimate Interests**: Processing is necessary for the purposes of legitimate interests pursued by Alpha Training or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

7. Data Subject Rights

Under GDPR, data subjects have the following rights:

- **Right to be Informed**: Individuals have the right to be informed about the collection and use of their personal data.
- **Right of Access**: Individuals have the right to access their personal data and supplementary information.
- **Right to Rectification**: Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.
- **Right to Erasure**: Individuals have the right to have personal data erased, also known as the "right to be forgotten."
- **Right to Restrict Processing**: Individuals have the right to request the restriction or suppression of their personal data.
- **Right to Data Portability**: Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- **Right to Object**: Individuals have the right to object to processing based on legitimate interests, direct marketing, and processing for research or statistical purposes.

- **Rights related to Automated Decision Making and Profiling**: Individuals have rights concerning automated decision-making and profiling.

8. Data Collection

Alpha Training collects personal data through various means, including but not limited to:

- Application forms and registration processes for learners.
- Employment and volunteer applications for staff and volunteers.
- Communications and interactions with learners, staff, and visitors.
- Online platforms and systems used for educational and administrative purposes.

8.1. Types of Personal Data Collected

- **Learners**: Name, date of birth, contact details, emergency contact information, educational records, health information, and attendance data.
- **Staff**: Name, contact details, employment history, payroll information, and performance records.
- **Visitors**: Name, contact details, and purpose of visit.
- **Other**: Any other data necessary for operational purposes or provided by individuals.

9. Data Processing

Alpha Training processes personal data for the following purposes:

- **Educational Services**: Delivering educational programs, monitoring learner progress, and managing learner records.
- **Administration**: Managing staff records, payroll, and recruitment processes.
- **Health and Safety**: Ensuring the health, safety, and well-being of learners, staff, and visitors.
- **Communication**: Facilitating communication with learners, staff, parents, and other stakeholders.
- **Compliance**: Meeting legal and regulatory obligations.

10. Data Sharing

Alpha Training will only share personal data with third parties where necessary for the purposes of processing, including:

- **Educational Authorities**: For compliance with educational regulations and funding requirements.
- **Healthcare Providers**: In cases where health information is required for safeguarding and welfare purposes.
- **External Contractors**: For services such as IT support, payroll, or other operational needs, under strict data protection agreements.
- **Law Enforcement**: When required by law or necessary for safeguarding purposes.

10.1. Third-Party Contracts

- **Data Processors**: Ensure that all third-party data processors comply with GDPR and have appropriate data protection agreements in place.

- **Due Diligence**: Conduct due diligence on all third-party processors to verify their data protection practices.

11. Data Security

Alpha Training implements appropriate technical and organisational measures to ensure data security, including:

- **Access Controls**: Limiting access to personal data to authorised individuals only.
- **Encryption**: Encrypting sensitive personal data both in transit and at rest.
- **Physical Security**: Securing premises and systems to prevent unauthorised access or data loss.
- **Data Breach Procedures**: Establishing procedures to detect, report, and investigate data breaches promptly.

12. Data Retention

Alpha Training retains personal data only for as long as necessary for the purposes for which it was collected, and in accordance with legal and regulatory requirements. Specific retention periods are outlined in the Data Retention Schedule.

12.1. Data Retention Schedule

- **Learner Records**: Retained for [insert time period] after the learner leaves Alpha Training.
- **Staff Records**: Retained for [insert time period] after employment ends.
- **Financial Records**: Retained for [insert time period] as required by law.
- **Health and Safety Records**: Retained for [insert time period] following the relevant incident or report.

13. Data Breach Management

In the event of a data breach, Alpha Training will:

- **Immediate Response**: Act swiftly to contain the breach and minimise impact.
- **Notification**: Notify the Information Commissioner's Office (ICO) within 72 hours if the breach poses a risk to data subjects.
- **Communication**: Inform affected data subjects if the breach is likely to result in a high risk to their rights and freedoms.
- **Investigation**: Conduct a thorough investigation to determine the cause of the breach and implement measures to prevent future occurrences.

14. Training and Awareness

Alpha Training is committed to ensuring that all staff members are aware of their data protection responsibilities and receive appropriate training:

- **Induction Training**: All new staff members receive training on GDPR and data protection policies as part of their induction.
- **Ongoing Training**: Regular updates and refresher sessions to keep staff informed of changes in data protection law and best practices.

- **Awareness Campaigns**: Promoting data protection awareness through workshops, bulletins, and resources available to all staff and learners.

15. Accountability and Governance

Alpha Training ensures accountability and governance by:

- **Data Protection Officer (DPO)**: Appointing a DPO responsible for overseeing data protection compliance, providing advice, and serving as the point of contact for data protection queries.
- **Data Protection Impact Assessments (DPIAs)**: Conducting DPIAs for high-risk processing activities to assess and mitigate potential risks.
- **Record Keeping**: Maintaining records of processing activities, including data categories, purposes, and retention periods.

15.1. Data Protection Officer (DPO)

Role and Responsibilities:

- **Monitor Compliance**: The DPO will monitor ongoing compliance with data protection laws, including regular audits and reviews of data processing activities.
- **Advise on Data Protection Matters**: Provide advice to the organisation and its employees on data protection obligations and best practices.
- **Point of Contact**: Serve as the primary point of contact for any queries or concerns regarding data protection and liaise with the Information Commissioner's Office (ICO) as necessary.
- **Training and Awareness**: Ensure that training programs on data protection are up-to-date and delivered effectively across the organisation.

15.2. Data Protection Impact Assessments (DPIAs)

When DPIAs are Required:

- **High-Risk Processing**: DPIAs are mandatory for any data processing activities that are likely to result in a high risk to the rights and freedoms of individuals, such as the introduction of new technologies, large-scale processing, or processing of sensitive data.

DPIA Process:

1. **Identify the Need for a DPIA**: Assess whether a DPIA is required for any new project or processing activity.
2. **Describe the Processing**: Clearly outline the nature, scope, context, and purposes of the processing.
3. **Consult Stakeholders**: Engage with relevant stakeholders, including the DPO, to gather input and assess risks.
4. **Assess Necessity and Proportionality**: Evaluate the necessity and proportionality of the processing activities.
5. **Identify and Assess Risks**: Identify potential risks to data subjects' rights and freedoms and assess their severity and likelihood.
6. **Mitigate Risks**: Implement measures to mitigate identified risks, ensuring they are proportionate to the risks involved.

7. **Document the DPIA**: Maintain a record of the DPIA process and outcomes, documenting decisions and any actions taken.
8. **Review and Update**: Regularly review DPIAs to ensure ongoing compliance and address any changes in processing activities.

15.3. Record Keeping

Processing Activities:

- **Data Inventory**: Maintain a comprehensive inventory of personal data held by Alpha Training, including categories of data subjects, types of data collected, purposes for processing, and retention periods.

Records Management:

- **Documentation**: Keep detailed records of data processing activities, ensuring they are accurate, up-to-date, and compliant with GDPR requirements.
- **Retention and Disposal**: Implement procedures for the secure retention and disposal of records in accordance with the data retention schedule.

16. Data Transfers

16.1. Transfers Outside the European Economic Area (EEA)

Lawful Transfers:

- **Adequacy Decisions**: Alpha Training will only transfer personal data to countries outside the EEA that have been deemed by the European Commission to provide an adequate level of data protection.
- **Appropriate Safeguards**: In the absence of an adequacy decision, transfers will only occur where appropriate safeguards are in place, such as standard contractual clauses, binding corporate rules, or other lawful mechanisms.
- **Explicit Consent**: In some cases, transfers may occur based on the explicit consent of the data subject, provided they have been informed of potential risks.

Transfer Procedures:

- **Assessment**: Conduct thorough assessments of potential risks associated with data transfers outside the EEA.
- **Approval**: Obtain approval from the DPO before initiating any transfers outside the EEA.
- **Documentation**: Document all data transfers, including the legal basis for the transfer and any safeguards implemented.

17. Data Protection by Design and by Default

17.1. Principles

Alpha Training is committed to implementing data protection by design and by default in all aspects of its operations:

- **Privacy by Design**: Integrating data protection principles into the design and development of systems, processes, and services from the outset.
- **Privacy by Default**: Ensuring that, by default, only the minimum necessary personal data is collected and processed, with privacy settings configured to the highest level.

17.2. Implementation

Design and Development:

- **Impact Assessments**: Conduct privacy impact assessments during the design phase of new systems or services to identify and mitigate potential privacy risks.
- **Data Minimisation**: Ensure that systems and processes are designed to collect and process only the data necessary for specified purposes.

Default Settings:

- **Access Controls**: Implement access controls and permissions to restrict access to personal data to authorised individuals only.
- **Data Collection**: Configure data collection settings to default to the least intrusive options, requiring explicit user action for additional data collection.

18. Review and Updates

18.1. Policy Review

Frequency:

- This GDPR policy will be reviewed annually to ensure ongoing compliance with legal requirements and best practices.

Trigger Events:

- Reviews will also occur in response to significant changes in legislation, organizational practices, or following data protection incidents.

Responsible Party:

- The Data Protection Officer, in conjunction with senior leadership, is responsible for reviewing and updating this policy.

18.2. Updates

Policy Amendments:

- Any updates or amendments to the policy will be communicated to all staff, learners, and relevant stakeholders promptly.

Training and Guidance:

- Revised training materials and guidance will be provided to ensure continued compliance with updated policy requirements.

19. Compliance and Enforcement

19.1. Compliance Monitoring

Audits and Assessments:

- Conduct regular audits and assessments to evaluate compliance with data protection policies and procedures.
- Implement corrective actions and improvements as necessary based on audit findings.

Reporting:

- Regular compliance reports will be submitted to senior leadership to ensure transparency and accountability.

19.2. Enforcement

Disciplinary Actions:

- Non-compliance with this policy may result in disciplinary actions, including training, warnings, or more severe consequences, depending on the nature and severity of the breach.

Incident Response:

- Establish procedures for responding to data protection incidents, including investigation, containment, and remediation.