SAFER RECRUITMENT 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 ensuring the safety and security of all employees, learners, visitors, volunteers, and assets. This Security Policy outlines our approach to managing security risks and establishing a secure environment for all individuals involved with the organisation.

2. Purpose

The purpose of this policy is to:

- Protect the physical security of all individuals on Alpha Training premises.
- Safeguard the organisation's assets, including buildings, equipment, data, and information systems.
- Ensure compliance with relevant security legislation and best practices.
- Establish clear roles, responsibilities, and procedures for security management.

3. Scope

This policy applies to:

- All Alpha Training employees, learners, visitors, volunteers, and contractors.
- All facilities and locations operated by Alpha Training, including the woodland lodge classroom, office, kitchen, toilet, practical animal room, stables, tack room, feed room, outdoor animal enclosures, and chicken sheds.
- All information systems and data, including electronic and paper-based records.

4. Security Principles

Alpha Training's security practices are based on the following principles:

1. **Proactive Risk Management**: We will identify, assess, and manage security risks proactively to minimise threats and vulnerabilities.
2. **Comprehensive Protection**: We will protect all assets, including people, property, and information, from theft, damage, and unauthorised access.
3. **Compliance and Integrity**: Our security practices will comply with all relevant legislation, regulations, and ethical standards.
4. **Continuous Improvement**: We will regularly review and improve our security measures to address emerging threats and ensure ongoing effectiveness.

5. Roles and Responsibilities

5.1. Senior Leadership Team (SLT)

- Oversee the implementation of security policies and procedures.
- Ensure adequate resources are allocated for security management.
- Monitor and review security performance and incidents.

5.2. Security Officer

- **Name**: Michelle Howdle

Responsibilities:

- Develop, implement, and review security policies and procedures.
- Conduct regular security risk assessments and audits.
- Manage security incidents and investigations.
- Provide training and guidance on security practices.

5.3. Employees and Volunteers

- Comply with security policies and procedures.
- Report any security incidents, concerns, or suspicious activities.
- Protect confidential information and assets.

5.4. Learners

- Follow security instructions and rules.
- Report any security concerns to staff immediately.
- Adhere to access control procedures.

5.5. Contractors and Visitors

- Comply with Alpha Training's security policies and procedures.
- Report any security concerns or incidents to a staff member immediately.

6. Physical Security

6.1. Access Control

- **Entry Points**: Secure all entry points with locks, access cards, or keypads. Ensure they are monitored and controlled to prevent unauthorised access.
- **Visitor Management**: Implement a visitor management system requiring visitors to sign in and wear identification badges.
- **Identification**: Issue identification badges for all staff, learners, and authorised personnel.
- **Restricted Areas**: Limit access to sensitive areas (e.g., data rooms, server rooms, and feed rooms) to authorised personnel only.

6.2. Surveillance Systems

- **CCTV Monitoring**: Install and maintain a closed-circuit television (CCTV) system to monitor key areas, including entrances, exits, and perimeters.
- **Signage**: Display clear signage indicating the use of CCTV for security purposes.
- **Data Protection**: Ensure CCTV footage is stored securely and access is restricted to authorised personnel only, in compliance with data protection laws.

6.3. Security Patrols

- **Regular Patrols**: Conduct regular security patrols of the premises, especially during off-hours or when the site is unoccupied.
- **Incident Reporting**: Document and report any incidents, hazards, or suspicious activities observed during patrols.

6.4. Lighting

- **Adequate Lighting**: Ensure that all areas, including entrances, exits, and parking lots, are well-lit to deter criminal activity and enhance safety.
- **Emergency Lighting**: Install emergency lighting systems to maintain visibility during power outages or emergencies.

6.5. Security of Buildings and Property

- **Lock and Secure**: Ensure all buildings, rooms, and equipment are locked and secured when not in use.
- **Maintenance**: Regularly maintain and inspect locks, doors, windows, and security systems to ensure functionality and effectiveness.
- **Asset Management**: Implement an asset management system to track and protect valuable equipment and resources.

7. Information Security

7.1. Data Protection

- **Data Classification**: Classify data according to sensitivity and implement appropriate protection measures.
- **Access Control**: Restrict access to data based on role and need, ensuring only authorised personnel can access sensitive information.
- **Encryption**: Use encryption for sensitive data in transit and at rest to prevent unauthorised access.

7.2. Network Security

- **Firewall and Antivirus**: Install and regularly update firewall and antivirus software to protect against cyber threats.
- **Secure Connections**: Use secure connections (e.g., VPNs) for remote access to the organisation's network and data.
- **Monitoring**: Monitor network traffic for suspicious activities and respond to potential threats promptly.

7.3. Password Management

- **Strong Passwords**: Enforce the use of strong passwords that meet complexity requirements.
- **Password Changes**: Require regular password changes and prompt updates following security breaches.

- **Multi-Factor Authentication**: Implement multi-factor authentication for accessing sensitive systems and data.

7.4. Information Handling and Storage

- **Confidentiality**: Ensure that sensitive information is handled and stored securely, both physically and electronically.
- **Data Retention**: Follow data retention and disposal policies to securely dispose of outdated or unnecessary data.
- **Training**: Provide training on data protection and information security practices for all staff and learners.

8. Emergency Procedures

8.1. Emergency Response Plan

- **Development**: Develop and implement an emergency response plan outlining procedures for various emergencies, including fire, medical incidents, and security breaches.
- **Communication**: Establish clear communication channels and responsibilities during emergencies.
- **Evacuation Drills**: Conduct regular evacuation drills to ensure preparedness and familiarity with emergency procedures.

8.2. Fire Safety

- **Fire Detection**: Install and maintain fire detection systems, including smoke detectors and alarms.
- **Fire Equipment**: Ensure fire extinguishers and other firefighting equipment are available and accessible.
- **Evacuation Routes**: Clearly mark and maintain evacuation routes and assembly points.

8.3. Incident Reporting and Investigation

- **Reporting**: Establish a system for reporting security incidents, including theft, vandalism, or breaches.
- **Investigation**: Investigate incidents promptly to identify causes, prevent recurrence, and implement corrective actions.

9. Training and Awareness

- **Security Training**: Provide regular training on security practices, emergency procedures, and data protection for all staff, learners, and volunteers.
- **Awareness Campaigns**: Conduct awareness campaigns to reinforce security policies and practices.

10. Monitoring and Review

10.1. Monitoring

- **Security Audits**: Conduct regular security audits and inspections to evaluate the effectiveness of security measures and identify areas for improvement.
- **Performance Metrics**: Monitor security performance metrics to assess compliance and identify trends or issues.

10.2. Review

- **Policy Review**: Review this policy annually or following significant changes in security requirements or incidents.
- **Updates**: Update security measures and procedures to reflect changes in legal requirements, threats, and best practices.

11. Compliance and Accountability

- **Legal Compliance**: Ensure compliance with all relevant security legislation, regulations, and standards.
- **Accountability**: Hold all individuals accountable for adhering to security policies and procedures, implementing disciplinary actions where necessary.

12. Associated Policies and Documents

- **GDPR Policy**
- **Health and Safety Policy**
- **Safeguarding Policy**
- **Data Protection Policy**

13. Legal Framework

- **Data Protection Act 2018 / GDPR**
- **Health and Safety at Work Act 1974**
- **Regulation of Investigatory Powers Act 2000**
- **Human Rights Act 1998**
- **Computer Misuse Act 1990**

14. Conclusion

Alpha Training is committed to maintaining a secure and safe environment for all individuals involved with our organisation. By adhering to this policy, we aim to protect our people, assets, and information while fostering a culture of security awareness and vigilance.