Information Governance & Data Management Policy

NextStep Training Ltd

1. Purpose

This policy outlines how NextStep Training Ltd manages information assets, including personal and confidential data. It ensures that data is processed legally, securely, and efficiently, supporting our commitment to transparency, accountability, and high standards of data protection.

2. Scope

This policy applies to:

- All staff, contractors, temporary workers, and volunteers.
- All learners, clients, and partners providing or receiving data.
- All systems and media (paper and electronic) used to collect, store, or process data.

3. Policy Statement

NextStep Training Ltd is committed to protecting the confidentiality, integrity, and availability of information. The organization ensures all personal data is:

- Processed fairly, lawfully, and transparently.
- Collected for specified and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and up to date.
- Retained only as long as necessary.
- Secured against loss, damage, or unauthorized access.

4. Legal and Regulatory Framework

This policy complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Human Rights Act 1998
- Education and Skills Funding Agency (ESFA) Guidelines
- Ofsted Data Handling Requirements (if applicable)

5. Roles and Responsibilities

Managing Director:

Has ultimate responsibility for compliance and oversight.

Data Protection Officer (DPO):

- Advises on data protection obligations.
- Monitors compliance and provides training.
- Handles data breaches and subject access requests (SARs).

All Employees and Contractors:

- Must follow this policy and attend data protection training.
- Must report breaches or concerns immediately.

6. Data Classification

All data is classified as:

- Public: Information intended for public access.
- Internal: Non-sensitive internal data.
- Confidential: Personal, learner, or staff information.
- Restricted: Highly sensitive data requiring strict controls.

7. Data Collection and Use

NextStep Training Ltd collects data for purposes including:

- Learner enrolment and course administration.
- Employment and HR processes.
- Funding, compliance, and reporting.
- Quality assurance and improvement.

All data subjects are informed about how their data is used via a Privacy Notice.

8. Data Storage and Security

- Data is stored securely on encrypted systems with password protection.
- Paper records are kept in locked cabinets with limited access.
- Access to data is role-based and monitored.
- Data backups are performed regularly and securely.
- Use of removable media is restricted and monitored.

9. Retention and Disposal

- Data is retained only as long as necessary and in line with the Data Retention Schedule.
- Secure disposal methods include shredding, secure digital deletion, and certified disposal services.

10. Subject Access Requests (SARs)

- Individuals have the right to access personal data held about them.
- Requests must be responded to within one calendar month.
- Requests should be submitted in writing to the DPO.
- Identity verification is required before processing.

11. Data Breaches

- Any suspected or actual data breach must be reported immediately to the DPO.
- The DPO will assess, record, and, if necessary, report the breach to the Information Commissioner's Office (ICO) within 72 hours.

12. Training and Awareness

- All employees must complete data protection training during induction and refresh it annually.
- Additional guidance is provided for those handling sensitive or large-scale data.

13. Third-Party Data Sharing

- Data will only be shared with third parties under a written agreement, ensuring GDPR compliance.
- Data sharing is limited to what is necessary for the specified purpose.
- Examples include funding bodies (e.g., ESFA), auditors, and awarding organizations.

14. Monitoring and Review

- The DPO and senior leadership will monitor compliance and perform periodic audits.
- This policy is reviewed annually or following significant legal, organizational, or technological changes.

15. Contact and Further Information
Data Protection Officer:
Name: Zak Vesamia
Email: zak@nextsteptrainingltd.co.uk
Phone: 020 7247 5497

Management Approval

Date: 19/02/2025

Managing Director