

Information Governance and Data Management Policy 2026-27

NextStep Training Ltd (NST)

Document control

This is Version 2.0 of the policy for 2026-27. It replaces the version updated in February 2025. It has been updated for the Data (Use and Access) Act 2025, the transfer of the Education and Skills Funding Agency's work to the Department for Education, and NST's current roles, and aligned with the Data Protection and Confidentiality Policy 2026-27.

Version	Date	Author	Authorised by	Next review
2.0	21 October 2026	Zak Vesamia (Data Protection Officer)	Ahmed Khan, Managing Director	21 October 2027
1.x	19 February 2025	—	Ahmed Khan, Managing Director	February 2026

Next review date: 21/10/2027

Approval: This policy has been reviewed and approved by:

Name: **AHMED KHAN**

Title: **Managing Director**

Signature: 

Date: 21/10/2026

1. Purpose

This policy sets out how NST manages its information assets, including personal and confidential data. It makes sure data is processed lawfully, securely and efficiently, supporting our commitment to transparency, accountability and high standards of data protection. It should be read with the Data Protection and Confidentiality Policy, the Staff Acceptable Use Policy and the Safeguarding, Child Protection and Prevent Policy.

2. Scope

This policy applies to:

- all staff, governors, contractors, temporary workers and volunteers
- all apprentices, learners, employers, clients and partners who provide or receive data
- all systems and media, paper and electronic, used to collect, store or process data, including cloud services, learning platforms and AI tools

3. Policy statement

NST is committed to protecting the confidentiality, integrity and availability of information. All personal data is:

- processed lawfully, fairly and transparently
- collected for specified and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- retained only as long as necessary
- secured against loss, damage or unauthorised access

4. Legal and regulatory framework

This policy complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
- Privacy and Electronic Communications Regulations 2003
- Computer Misuse Act 1990
- Human Rights Act 1998
- Equality Act 2010
- Department for Education apprenticeship funding rules 2026 to 2027, including data and evidence requirements (the Education and Skills Funding Agency closed on 31 March 2025 and its work moved to the DfE)
- Ofsted inspection requirements for data and records
- Keeping Children Safe in Education 2026, for safeguarding records and information sharing

5. Roles and responsibilities

Role	Responsibilities
Managing Director (Ahmed Khan)	Ultimate responsibility for compliance and oversight; reports to the Board of Governors
Data Protection Officer (Zak Vesamia)	Advises on data protection obligations; monitors compliance and provides training; handles data breaches, subject access requests and data protection complaints
MIS and Compliance (Sayed Nafis, Marihah Askor)	Manages learner records and ILR data quality; system security, access controls and backups; evidence storage
All employees and contractors	Follow this policy and complete data protection training; report breaches or concerns immediately

6. Data classification

Class	Meaning
Public	Information intended for public access, such as course information on NST's website
Internal	Non-sensitive internal information, such as staff procedures
Confidential	Personal information about apprentices, employers and staff
Restricted	Highly sensitive information needing strict controls, such as safeguarding records, health and special category data

7. Data collection and use

NST collects data for purposes including:

- apprentice recruitment, enrolment and programme administration
- teaching, assessment, progress reviews and end-point assessment
- safeguarding and learner support
- employment and HR processes
- funding claims, compliance and reporting to the Department for Education (Individualised Learner Record)
- quality assurance and improvement

Everyone whose data NST collects is told how it is used through a privacy notice.

8. Data storage and security

- Data is stored securely on encrypted, password-protected systems, with multi-factor authentication where available.
- Paper records are kept in locked cabinets with limited access.
- Access to data is role-based and monitored.

- Backups are made regularly and securely, and tested.
- Removable media are restricted and must be encrypted.
- Only approved systems and AI tools may be used for NST data.

9. Retention and disposal

- Data is kept only as long as necessary, in line with NST's Data Retention Schedule and the DfE's funding and audit requirements.
- Safeguarding records are kept for the periods set out in the Safeguarding, Child Protection and Prevent Policy.
- Secure disposal includes cross-cut shredding, secure digital deletion and certified disposal services.

10. Subject access requests

- Individuals have the right to access personal data held about them, free of charge.
- Requests are answered without undue delay and within one calendar month, extendable by up to two months for complex requests.
- Requests can be made in any form and should be passed to the Data Protection Officer straight away.
- Identity is verified before information is released.

11. Data breaches

- Any suspected or actual breach must be reported to the Data Protection Officer immediately.
- The Data Protection Officer assesses and records it and, where required, reports it to the Information Commissioner's Office within 72 hours.

12. Data protection complaints

Complaints about how NST uses personal data are handled under the data protection complaints procedure in the Data Protection and Confidentiality Policy, in force from 19 June 2026: complaints are acknowledged within 30 days and investigated without undue delay.

13. Training and awareness

- All staff complete data protection training at induction and refresh it every year.
- Additional guidance is given to those handling sensitive or large-scale data, such as MIS and safeguarding staff.

14. Third-party data sharing

- Data is shared with third parties only where there is a lawful basis and, where required, a written agreement that makes sure the data is protected.
- Sharing is limited to what is necessary for the purpose.
- Examples include the Department for Education, awarding and end-point assessment organisations, employers, auditors and, for safeguarding, social care and the police.

15. Monitoring and review

- The Data Protection Officer and senior leadership monitor compliance and carry out periodic audits, reporting to the Board of Governors.
- This policy is reviewed every year, or sooner after significant legal, organisational or technological change.

16. Contact

Data Protection Officer: Zak Vesamia · zak@nextsteptrainingltd.co.uk · 020 7247 5497