

Data Protection and Confidentiality Policy 2026-27

NextStep Training Ltd (NST) · ICO registration number Z2884210

Document control

This is Version 4.0 of the policy for 2026-27. It replaces Version 3.2 (February 2025). It has been updated to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, replacing out-of-date references to the Data Protection Act 1998, subject access fees and European Economic Area transfers, and adds the data protection complaints procedure required from 19 June 2026.

Version	Date	Author	Authorised by	Next review
4.0	21 October 2026	Zak Vesamia (Data Protection Officer)	Ahmed Khan, Managing Director	21 October 2027
3.2	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. Introduction

NST takes its data protection responsibilities very seriously. This policy sets out how we meet them.

NST collects, uses, stores and otherwise processes personal data about apprentices and other learners (past, present and prospective), employers and their staff, NST staff, governors, contractors, volunteers, suppliers, website users and other contacts ("data subjects"). When we do so, we must respect people's reasonable expectations of privacy and comply with data protection law.

This policy makes sure that we:

- are clear about how personal data must be processed, and what we expect of everyone who processes it on our behalf
- comply with data protection law and follow good practice
- protect people's rights and NST's reputation
- protect NST from the risk of personal data breaches and other breaches of data protection law

2. The law

The UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, set out how organisations must collect, handle and store personal data, whether it is held electronically, on paper or in any other form. Under Article 5 of the UK GDPR, personal data must be:

1. processed lawfully, fairly and in a transparent way
2. collected for specified, explicit and legitimate purposes, and not used in ways incompatible with them
3. adequate, relevant and limited to what is necessary
4. accurate and, where necessary, kept up to date
5. kept for no longer than necessary
6. kept secure, protected against unauthorised or unlawful processing, accidental loss, destruction or damage

NST must also be able to show that it complies with these principles (accountability).

NST only processes personal data where it has a lawful basis, such as a contract, a legal obligation (for example funding and safeguarding duties), a public task, legitimate interests or, where needed, consent. Special category data, such as health, ethnicity, disability and religion, and criminal offence data are processed only where the law allows, for example for safeguarding, equality monitoring or funding requirements, and with extra protection.

3. Scope

This policy applies to:

- NST's office in Hackney, apprentices' workplaces when NST staff are there, remote and online working, and any other location where NST data is used
- all staff, governors, contractors, suppliers and volunteers working for NST
- all apprentices, learners, employers and clients involved with NST

It covers all personal data NST holds about identifiable individuals, including names, addresses, email addresses, phone numbers, dates of birth, national insurance numbers, learning and assessment

records, equality and support needs, safeguarding records, employment records, photographs and recordings, and any other information relating to individuals.

4. Data protection risks

- **Breaches of confidentiality**, for example information being given out inappropriately or sent to the wrong person
- **Failing to respect people's rights**, for example not being transparent about how data is used
- **Cyber attacks and data loss**, for example phishing, ransomware or lost devices
- **Reputational and financial damage** if data is lost or misused

5. Responsibilities

Everyone who works for or with NST is responsible for making sure personal data is collected, stored and handled appropriately and in line with this policy.

Role	Responsibilities
Board of Governors and Managing Director (Ahmed Khan)	Overall responsibility for NST meeting its legal obligations; approving this policy; receiving reports on data protection risks, breaches and complaints
Data Protection Officer (Zak Vesamia)	Advising the Board and staff on data protection; reviewing procedures and policies; arranging training; handling subject access and other rights requests; handling data protection complaints; managing data breaches and reporting them to the ICO; checking contracts with third parties that process NST data
MIS and Compliance (Sayed Nafis, Mariyah Askor)	Making sure systems and equipment meet appropriate security standards; regular security checks and backups; evaluating third-party and cloud services before use; keeping learner records accurate and secure
Business Development (Laura Stephens Nield)	Making sure marketing follows data protection and electronic marketing rules, including checking marketing lists against suppression files at least every 6 months
All staff	Following this policy; completing data protection training at induction and every year; reporting breaches or concerns immediately

6. General staff guidelines

- Only people who need personal data for their work may access it. Access is role-based.
- Do not share personal data informally. If you need access to confidential information, ask your line manager.
- Use strong passwords and multi-factor authentication where available, and never share them.
- Do not disclose personal data to unauthorised people, inside or outside NST.
- Review data regularly; update it when it is out of date and securely delete it when it is no longer needed, in line with the Data Retention Schedule.
- Ask the Data Protection Officer if you are unsure about any aspect of data protection.

- Data protection law never prevents sharing information needed to keep a child or adult at risk safe. Safeguarding information is shared in line with the Safeguarding, Child Protection and Prevent Policy.

7. Data storage

- Paper records are kept in locked cabinets in NST's office and never left where others can see them, for example on a printer. Paper no longer needed is shredded or disposed of through a secure service.
- Electronic data is protected from unauthorised access, accidental deletion and hacking by strong passwords, encryption, security software and a firewall.
- Store data only on NST's approved systems and cloud services. Do not save personal data to the local drive of a laptop, tablet or phone, or to personal accounts.
- Removable media are not used for personal data unless encrypted and agreed by the Data Protection Officer.
- Data is backed up frequently, and backups are tested regularly.

8. Data use and sharing

- Lock your screen whenever you leave your device unattended.
- Send personal data only through secure, approved methods, such as NST's secure systems or encrypted email. Check the recipient before sending.
- Share personal data with third parties, such as the Department for Education, awarding and end-point assessment organisations, employers and auditors, only where there is a lawful basis and, where required, a written agreement.
- Do not enter personal data into AI tools that NST has not approved.
- Personal data is transferred outside the UK only where the law allows, for example to a country with UK adequacy regulations or with appropriate safeguards in place. Check with the Data Protection Officer first.

9. Data accuracy

NST must take reasonable steps to keep data accurate and up to date. Staff should hold data in as few places as necessary, avoid creating unnecessary extra data sets, take every opportunity to check details (for example when an apprentice calls), and correct inaccuracies as soon as they are found.

10. Individuals' rights

Everyone whose personal data NST holds has rights under data protection law, including the right to:

- be told how their data is used (NST's privacy notices)
- access their data (a subject access request)
- have inaccurate data corrected
- have data erased or its use restricted in some circumstances
- object to some uses of their data, including direct marketing
- data portability, where it applies
- complain to NST and to the Information Commissioner's Office

Subject access requests

- Requests can be made in any form, including verbally, but it helps to email info@nextsteptrainingltd.co.uk, marked for the attention of the Data Protection Officer. A standard form is available but does not have to be used.
- NST verifies the identity of anyone making a request before releasing information.
- There is no fee. NST may charge a reasonable fee, or refuse, only where a request is manifestly unfounded or excessive.
- NST responds without undue delay and within one month. For complex or multiple requests, this can be extended by up to two further months, and we will tell the person why within the first month.
- NST carries out reasonable and proportionate searches for the information requested.

11. Data protection complaints

From 19 June 2026, the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025) requires NST to have a process for handling complaints about how it uses personal data. Anyone can complain to NST, in any form, including by email to info@nextsteptrainingltd.co.uk or by phone on 020 7247 5497. NST will:

- acknowledge the complaint within 30 days of receiving it
- investigate without undue delay, in a way that is reasonable and proportionate to the issues raised
- keep the person informed of progress and any delays
- tell them the outcome without undue delay

Privacy notices, and responses to rights requests, tell people about this right. If they remain unhappy, they can complain to the Information Commissioner's Office (ico.org.uk, 0303 123 1113).

12. Personal data breaches

Any suspected or actual data breach, such as a lost device, an email sent to the wrong person or a cyber attack, must be reported to the Data Protection Officer immediately. The Data Protection Officer assesses and records every breach and, where it is likely to result in a risk to people's rights and freedoms, reports it to the ICO within 72 hours of NST becoming aware of it. Where the risk is high, the people affected are told without undue delay.

13. Disclosing data for other reasons

In some circumstances, the law allows personal data to be disclosed without the person's consent, for example to the police to prevent or detect crime, or to children's or adult social care to keep someone safe. The Data Protection Officer makes sure the request is legitimate, seeking advice from the Managing Director and NST's legal advisers where necessary, and records the decision.

14. Providing information

NST makes sure people know how their data is used and how to exercise their rights, through privacy notices for apprentices, employers, staff and website users. Privacy notices are available on request and on NST's website.

15. Training and review

All staff complete data protection training at induction and every year. This policy is reviewed every year, or sooner if the law, guidance or NST's systems change.

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