Vision Training North East

Data Protection Policy

Version: 2.4
Last Review: January 2026

Signed:

Policy Name	Data Protection Policy
Policy Owner	Data & ICT Lead
Copy Type	External Copy

Approvals

First Approved	January 2013
Governance Approved	Y
SMT Approved	Y

Applicable To /Accessible By

Employees	✓
Learners/Apprentices	✓
Employers	✓
Website Access	✓

Reviews

Scheduled Review Cycle	Annual
Responsible Manager(s)	Data & ICT Lead Data & ICT Deputy
Last Review Date	January 2026
Next Review Due By	January 2027
Current Version Number	V2.4

Data Protection Policy

1. Data Protection Policy Statement

Vision Training (North East) Ltd is committed to complying with all applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Data (Use and Access) Act 2025 (DUAA), and the Privacy and Electronic Communications Regulations 2003 (PECR) (as amended).

We will maintain proportionate procedures to ensure all employees and others acting on behalf of the organisation who handle personal data understand and comply with their duties under data protection law.

We will process personal data lawfully, fairly and transparently, and maintain appropriate technical and organisational measures to keep personal data secure.

2. Purpose

Vision Training (North East) Ltd must collect and use information about people with whom it works to operate and carry out its functions. This includes current, past, and prospective employees, apprentices and learners, clients, employers, and suppliers.

Personal information must be handled appropriately regardless of how it is collected, recorded and used, whether held on paper, electronically, or in any other format.

We regard the lawful and appropriate treatment of personal information as essential to maintaining trust and confidence. We therefore adhere to the UK GDPR principles and related duties, including:

1. Lawfulness, Fairness and Transparency
   We will process personal data fairly and transparently and will provide clear privacy information to individuals.

2. Purpose Limitation
   We will collect personal data for specified, explicit and legitimate purposes and not process it in a manner incompatible with those purposes.

3. Data Minimisation
   We will only collect personal data that is adequate, relevant and limited to what is necessary for the stated purposes.

4. Accuracy

We will take reasonable steps to ensure personal data is accurate and, where necessary, kept up to date. Where we are notified of inaccuracies, we will review and correct data without undue delay.

5. Storage Limitation
   We will not keep personal data for longer than necessary. Retention will be in line with the Data Retention Schedule and legal, contractual, and funding requirements.

6. Integrity and Confidentiality (Security)
   We will protect personal data against unauthorised or unlawful processing, and against accidental loss, destruction or damage, through appropriate security measures.

7. Accountability
   We will be able to demonstrate compliance through governance, records, training, risk assessment, and monitoring.

3. Scope

This policy applies to all employees and directors of Vision Training (North East) Ltd. It also applies to third parties where they process personal data on our behalf, under contract and instruction.

4. Definitions

4.1 Data, Personal Data and Data Subject

- Data is information processed by automated means or held in structured filing systems.
- Personal Data means any information relating to an identified or identifiable living individual, directly or indirectly, such as name, address, date of birth, postcodes, unique identification numbers, location data, and online identifiers.
- Data Subject means the individual to whom the personal data relates.

4.2 Special Category Data

Special category personal data includes information revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data, biometric data (where used for identification)
- health data

- sex life or sexual orientation.

4.3 DATA PROTECTION LEGISLATION

This includes:

1. UK General Data Protection Regulation ("UK GDPR"),
2. Data Protection Act 2018
3. Data Use and Access Act 2025 (DUAA)
4. Privacy and Electronic Communications Regulations 2003 (as amended), and
5. Any other applicable law relating to privacy and personal data processing.

4.4 GENERIC DATA ROLES

"data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

"data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

"processing", in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

1. organisation, adaptation or alteration of the information or data
2. retrieval, consultation or use of the information or data
3. disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data

5. Roles and Responsibilities

5.1 Directors

Directors are accountable for ensuring the organisation meets its legal responsibilities under data protection legislation, including ensuring appropriate resourcing, oversight, and effective controls.

5.2 Data & ICT Lead and Deputy

The Data & ICT Lead is the organisation's nominated Data Protection Lead and primary contact for data protection matters. The Deputy supports this role.

They are responsible for:

1. Ensuring all employees handling personal data receive appropriate training, guidance, and updates.
2. Providing advice and guidance on data protection compliance.
3. Acting as the primary point of contact for data subject requests.
4. Acting as the primary point of contact with the Information Commissioner's Office (ICO) where required.
5. Maintaining a log of data subject requests, outcomes, and reasons where requests are refused or limited.
6. Regularly reviewing, and where necessary updating, privacy notices and statements.
7. Supporting the organisation to identify and document lawful bases for processing, including where DUAA provisions apply.
8. Ensuring contracts with processors include required data protection clauses.
9. Overseeing breach management, investigations, and reporting decisions.
10. Supporting DPIAs (Data Protection Impact Assessments) where processing is likely to result in high risk.

5.3 Line Managers

Line Managers are responsible for:

- reinforcing this policy within their teams
- ensuring local working practices comply with this policy
- escalating concerns promptly to the Data & ICT Lead

5.4 All Employees

All employees must:

- Process personal data in line with this policy and current legislation.
- Complete data protection training as required.
- Report actual or suspected breaches or concerns to the Data & ICT Lead immediately.
- Only use personal data for the stated purpose(s) and within the lawful basis communicated to the data subject.
- Inform the Data & ICT Lead within 1 working day of any verbal data subject request received.

6. Data Protection Policy Implementation – Procedures

6.1 Data Subject Rights

6.1.1 Informing Data Subjects About Data Collection

Vision Training (North East) Ltd will provide privacy information at the time of collection, including:

- purposes and lawful basis for processing
- retention periods
- who it will be shared with
- the rights available to individuals and how to exercise them

Where personal data is obtained from another source (for example an employer or partner college), the Data & ICT Lead must be informed and privacy information will be provided within a reasonable period and no later than one month, unless a valid exemption applies.

6.1.2 Subject Access Requests (SARs)

Data subjects have the right to request access to their personal data.

- Requests must be processed within one month.
- Where requests are complex or numerous, the deadline may be extended by up to two further months, with an explanation issued within the initial one-month period.
- Identity verification may be required where reasonable and proportionate.
- Information will be provided unless an exemption applies (the Data & ICT Lead will advise).

Responses will include the required UK GDPR information, including purposes, categories, recipients, retention, rights, complaints route, source (if not collected from the individual), and international transfer safeguards where relevant.

6.1.3 Rectification

Individuals have the right to correct inaccurate personal data. Requests will be reviewed and responded to within one month. Where we refuse or limit a request, we will explain the reasons and signpost the individual's right to complain to the ICO.

6.1.4 Erasure (Right to be Forgotten)

Requests will be processed within one month. Where erasure is refused or limited due to legal obligations, public task, archiving exemptions, or legal claims, the Data & ICT Lead will explain the reason and signpost the ICO route.

6.1.5 Restriction

Where applicable, we will restrict processing while accuracy or lawful basis is being considered. Requests will be handled within one month, with reasons provided where refused or limited.

6.1.6 Data Portability

Where processing is based on consent or contract and carried out by automated means, we will provide data in a structured, commonly used and machine-readable format within one month, or explain why this does not apply.

6.1.7 Right to Object

We will respond within one month. Objections to direct marketing will be actioned immediately. Other objections will be assessed against our lawful basis and the individual's rights.

6.1.8 Automated Decision Making

Vision Training (North East) Ltd does not currently use automated decision making or profiling that produces legal or similarly significant effects.

6.2 Data Retention

Vision Training (North East) Ltd will not keep personal data for longer than necessary. Where practicable, data may be anonymised for statistical purposes. All employee must follow the Data Retention Schedule.

Please see also the data retention schedule

6.3 Data Security

6.3.1 Access Controls and Storage

1. Paper files must be secured when not in use. Electronic systems must be access controlled and protected, including multi-factor authentication where available.
2. Employees must prevent unauthorised viewing of personal data on screens or paper records, including when working remotely.
3. Electronic data must be stored only on approved organisational systems (for example OneDrive and associated managed Microsoft 365 services).
4. Personal data must not be stored on local desktops, unsecured removable media, or personal devices.
5. Devices must be locked when unattended. Passwords must not be shared.

6.3.2 Personal Data Breaches

A personal data breach is a security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

All employees must report suspected breaches to the Data & ICT Lead immediately.

The Data & ICT Lead will:

- investigate, contain and record the breach

- assess likelihood and severity of risk to individuals' rights and freedoms
- notify Directors
- notify the ICO without undue delay and within 72 hours where required
- notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms

All breaches, whether reportable or not, will be recorded in the breach log with rationale for decisions.

See further advice and guidance on the ICO website

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

6.4 Information Sharing

Information will only be shared where there is a lawful basis and it is necessary, proportionate, and secure.

We pass information to government agencies to meet funding requirements. Vision Training (North East) Ltd acts as a data processor for the Education and Skills Funding Agency (ESFA) in relevant contexts and will share required information for statutory and funding purposes, including maintaining Unique Learner Numbers (ULNs) and Personal Learning Records (PLRs), in line with data protection legislation.

We share learner information with awarding bodies for registration, quality assurance, administration and certification, and with partner organisations where necessary for delivery and administration, in line with lawful bases and information sharing agreements.

6.4.1 New or Changed Data Sharing

Any first-time or changed data sharing must be reviewed with the Data & ICT Lead prior to disclosure to confirm lawful basis, purpose, and appropriate safeguards.

6.4.2 Sharing Without Consent

Consent is not the only lawful basis for sharing. Personal data may be shared without consent where there is a valid lawful basis and, where applicable, a relevant exemption, including safeguarding, prevention or detection of crime, or compliance with a legal obligation. The Data & ICT Lead will advise on the lawful basis and documentation required.

6.5 SECURE TRANSFER OF DATA

Personal data transfers must be secure and limited to what is necessary. Recipient identity must be verified.

6.5.1 Electronic Transfers

- Do not include personal data in email subject lines.
- Use password-protected attachments or secure sharing links where appropriate, and send passwords separately.
- Do not use personal email accounts for personal data.

6.5.2 Paper-Based Transfers

Paper records containing personal data must be transferred securely to a named recipient, either by secure postal methods, in-person delivery, or secure scanned transfer.

6.6 THIRD PARTY SOFTWARE

We only use recognised suppliers where appropriate assurances and contractual controls are in place, including data processing agreements where required. Systems may include those used for e-portfolio, ILR management, awarding body registration, diagnostics, surveys and communications.

All new software or suppliers that process personal data must be approved via the Data & ICT Lead prior to use.

6.7 VISIONTRAININGNORTHEAST.COM WEBSITE

We use cookies on our website to support functionality and improve user experience. Cookie controls and privacy information must be provided in line with PECR and data protection requirements. Links to third party sites are outside our control and users are advised to review the privacy information of those sites.

6.8 COMPLAINTS ABOUT PERSONAL DATA

Individuals who wish to complain about how their personal data has been handled should be referred to the Data & ICT Lead in the first instance. If the complaint cannot be resolved, the individual has the right to complain to the ICO.

6.9 CONFIDENTIALITY

All employees must treat personal data as confidential and process it only in line with this policy and authorised procedures.

6.10 Training

All employees receive basic data protection training during induction and periodic updates thereafter, including refresher training as required by the Data & ICT Lead.

6.11 Related Policies & Documents

Confidentiality Policy; Data Retention Schedule; ICT Acceptable Use Policy: Information Security arrangements; Privacy Notices.

Common Addendum

Policy Review

The Policy & Procedure Lead is responsible for managing the annual review of the policy.

The manager(s) indicated on the first page are responsible for completing the annual review of the policy and communicating all necessary changes to the Policy and Procedure Lead. The owner will then sign off the policy once updates are complete.

The review can be delegated to another manager as part of their Professional development. However, the policy owner retains full responsibility for ensuring the policy:

- Complies with current legislation
- Meets the centre's responsibilities as
    - a lead independent training provider
    - a sub-contractor
    - a partner in line with funding and awarding bodies' requirements
- Supports stakeholders in implementing the policy effectively.

The Quality Lead ensures that all employees acknowledge policy updates through the Quarterly Policy Monitoring Form.

Policy Access, Communication and Promotion

Internal, all employees

All policies are accessible via the VTNE shared folder. Managers must communicate relevant policies to their teams and ensure employees:

- Read the policies during induction
- Receive guidance on responsibilities and implementation
- Receive necessary training, e.g. Health & Safety

- Sign to confirm their understanding

Policy updates are communicated via email, intranet, and team meetings.

The Data and ICT Lead ensures policies are accessible to learners and employers, either online or by request.

Promotion of the policy to learners and employers (where applicable)

Tutors: Ensure learners understand their responsibilities and deliver related activities (e.g., safeguarding, welfare).
Employer Engagement Lead: Promotes relevant policies to employers and ensures they understand their responsibilities.

Monitoring and Reporting

Line managers monitor policy compliance within their teams and address any issues as they arise. Employees have a clear process for reporting any concerns, which should be communicated by line managers.

1. Definitions For Policy Purposes

Please note that not all terms may be used within this policy.

Candidate(s): A person individual who has expressed an interest in a programme with Vision Training (North East) Limited but is not yet registered.

Learner(s): A registered learner on a short course or an apprentice learner registered on an apprenticeship with Vision Training (North East) Limited or a partner college.

Employer(s): The employer of a registered learner or candidate.

Employee(s): A person employed by Vision Training (North East) Limited.

The Centre: Vision Training (North East) Limited's Training Centre in Stockton-on-Tees and any current satellite offices.

Stakeholders: A member of one or more of the above groups relevant to the policy.

Appendix 1 – Lawful Bases for Processing

- You must have a valid lawful basis in order to process personal data.
- You must determine the lawful basis before you begin processing and this must be appropriately documented.
- No single basis is 'better' or more important than the others – which basis is most appropriate will depend on the purpose for processing and the council's relationship with the individuals concerned.

There are six available lawful bases for processing Personal Data:

- **Consent** – freely given, informed and evidenced by a clear affirmative action
- **Contract** – necessary for the performance of a contract with the Data Subject (inc. specific steps before entering into a contract)
- **Legal Obligation** – necessary to comply with the law
- **Vital Interests** – necessary to protect the life of the data subject
- **Public Task** – necessary to perform a task in the public interest or for the council's official functions, and the task or function has a clear basis in law.
- **Legitimate Interests** – necessary for the council's, or a third parties, legitimate interests in circumstances where the Data Subject's right to privacy does not override those legitimate interests (NB. This legal basis is unavailable for public authorities when the processing is in connection with an official task)

If you are processing Special Category Personal Data, you must also identify a further lawful basis. There are ten available lawful bases for processing Special Category Data:

- **Explicit Consent** – freely given, informed and evidenced by a clear affirmative action
- **Employment, social security or social protection law** – necessary to meet legal obligations in these specific areas
- **Vital Interests** – necessary to protect the life of the data subject or another individual where they are physically or legally incapable of giving consent
- **Not-for-profit Bodies** – processing carried out by a political, philosophical, religious or trade union
- **Deliberately made public by the Data Subject** – data that has manifestly been placed in the public domain by the Data Subject
- **Legal Claims** – necessary for establishing, exercising or defending legal rights.
- **Substantial Public Interest** – necessary for reasons of substantial public interest e.g. official functions, statutory purposes, equal opportunities or preventing or detecting unlawful acts.
- **Health and Social Care** – necessary to preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, provision of health or social care or treatment or management of health and social care systems
- **Public interest in the area of Public Health** – such as threats to health or ensuring high standards of healthcare
- **Archiving Purposes** – public interest, scientific and historical research purposes or statistical purposes.

Further lawful bases are available for processing Criminal Convictions Data and advice must be sought prior to processing to determine what the appropriate lawful basis is.

Appendix 2 – Privacy Statement/Notice Checklist

The following information must be supplied on every Privacy Statement/Notice:

- ✓ The name and contact details of our organisation.
- ✓ The name and contact details of our representative (if applicable).
- ✓ The contact details of our data protection officer (if applicable).
- ✓ The purposes of the processing.
- ✓ The lawful basis for the processing.
- ✓ The legitimate interests for the processing (if applicable).
- ✓ The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- ✓ The recipients or categories of recipients of the personal data.
- ✓ The details of transfers of the personal data to any third countries or international organisations (if applicable).
- ✓ The retention periods for the personal data.
- ✓ The rights available to individuals in respect of the processing.
- ✓ The right to withdraw consent (if applicable).
- ✓ The right to lodge a complaint with a supervisory authority.
- ✓ The source of the personal data (if the personal data is not obtained from the individual it relates to).
- ✓ The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- ✓ The details of the existence of automated decision-making, including profiling (if applicable)