Data Protection Policy

Reviewed by	Paul Shepherd
Signed off by	Gary Whaites
Date	January, 2026
Review Date	January, 2027

NSPP Data Protection Policy

Version: 3
Date Reviewed: January 2026
Next Review: January 2027

1. Introduction

NSPP Vocational Training is committed to full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We take seriously our responsibility to protect the personal data of learners, staff, employers, and stakeholders. This policy outlines how NSPP collects, stores, processes, and protects personal data, and how we respond to incidents involving data security.

2. Scope

This policy applies to all personal data held by NSPP in relation to its business operations, including learner records, staff information, third-party suppliers, and employer partners. It covers both electronic and paper-based records, and applies to all employees, contractors, and volunteers.

3. Key Definitions

- **Personal Data**: Any information relating to an identifiable individual.
- **Special Category Data**: Sensitive data including health, ethnicity, religious beliefs, or sexual orientation.
- **Data Subject**: The individual whom the personal data relates to.
- **Data Controller**: NSPP, which determines the purpose and means of processing personal data.
- **Data Processor**: A third party that processes personal data on behalf of NSPP.

4. Lawful Basis for Processing

NSPP processes personal data only where there is a lawful basis to do so. These include:

- Contractual obligations (e.g. funding agreements)
- Legal obligations (e.g. safeguarding)
- Legitimate interests (e.g. learner support)
- Consent (where required)

5. Data Subject Rights

NSPP upholds the following rights for data subjects:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing

- Right to data portability
- Right to object

Requests can be made in writing to NSPP's Data Protection Officer (DPO). We will respond within one calendar month.

6. Data Minimisation and Retention

We only collect data that is necessary for our operational and funding obligations. Personal data is retained in accordance with the Education and Skills Funding Agency (ESFA) requirements and NSPP's internal retention schedule. Once no longer required, data is securely deleted or destroyed.

7. Privacy Notices

All learners, staff, and partners are provided with a privacy notice explaining:

- What data is collected
- Why it is collected
- How it is used
- Who it is shared with
- How long it is retained

Privacy notices are issued at the point of data collection and are available on request.

8. Data Security

- All data is stored securely using encrypted systems and protected physical storage.
- Staff are trained in safe data handling, password security, and secure communications.
- Access to data is restricted based on role and business need.
- NSPP uses approved systems and follows ESFA and WMCA guidance on cyber and data security.

9. Data Sharing and Third Parties

Where data is shared with funding bodies, employers, or third-party services (e.g. CRM, MIS), contracts and data processing agreements are in place. Third parties are audited where appropriate to ensure compliance with UK GDPR.

10. Staff Responsibilities and Training

- All employees are responsible for the secure handling of personal data.
- Training is provided at induction and refreshed annually.
- Failure to follow data protection procedures may result in disciplinary action.

11. Information Security Incident Reporting

All actual or suspected data breaches must be reported immediately to the Data Protection Officer using the NSPP Information Security Incident Report Form (Appendix 1).

11.1 Initial Response

Upon receiving an incident report:

- The DPO will evaluate whether immediate containment is needed.
- Action may include securing data, equipment recovery, or contacting external services.

11.2 Investigation

- Incidents are investigated by the DPO, with input from relevant managers.
- Investigation outcomes are documented, and recommendations made to Senior Management.

11.3 Evaluation and Lessons Learned

We assess whether:

- The risk was previously identified
- Controls were adequate
- Staff followed procedures
- Policy updates or further training are needed

11.4 Notification

Depending on the breach, we may notify:

- The Information Commissioner's Office (ICO)
- Affected individuals
- Employers, funders, or other agencies

11.5 Disciplinary Action

Failure to comply with this policy may result in disciplinary action, including termination of employment.

12. Policy Governance

This policy is reviewed annually or in response to significant incidents or legislative changes. It is approved by Senior Management and made available to all staff.

Appendix 1: Examples of Information Security Incidents

- Loss or theft of a laptop or USB stick containing learner data
- Email sent to the wrong recipient containing personal details
- Use of unapproved software storing personal data
- Inappropriate access or sharing of learner records
- Printing or copying confidential information and failing to store it securely

Appendix 2: Information Security Incident Reporting Form

Please send the completed form to paul.shepherd@nspp.co.uk and DO NOT take any further action unless advised.

The incident will be investigated and where appropriate a report issued.

Employee Reporting Incident	
Person Responsible for Incident	
Date/Time of Incident	
Type of Data*	

*Examples of data

- Files/Paperwork containing personal data
- Data stored on an information system
- Emails stored on Laptop/iPad

Details of Incident
Describe in detail how the incident occurred.
Did the employee self-report the incident.

Are there any mitigating circumstances?
Outline which data is involved
Approximately how many individuals are affected?
Has the data been recovered?

Signed: Date:

When completed, please return to paul.shepherd@nspp.co.uk