

Data Protection Policy v7

1. Purpose

Any Driver Limited is committed to protecting the privacy and security of personal data.

This policy sets out how we comply with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Privacy and Electronic Communications Regulations (PECR)
- Department for Education (DfE) funding rules
- Student Loans Company (SLC) contractual requirements

We process personal data in connection with delivery of qualifications funded by the Department for Education and Advanced Learner Loans administered by the Student Loans Company.

Any Driver is registered with the Information Commissioner (www.ico.gov.uk) and has a Data protection Licence (DPL) Tier 1. Our registration is classed as an Information Processor which enables us to handle information relevant to our services and enable us to function as an employer.

Our ISO registration numbers is **ZA049069**, with a start date of 29th March 2014 and end date of 28th March 2027.

2. Scope

This policy applies to:

- Learners (including Advanced Learner Loan applicants)
- Staff and contractors
- Employers
- Governors/directors
- Visitors
- Third-party partners

It applies to all personal data processed by the Organisation in electronic or paper form.

3. Definitions

- **Personal Data:** Information relating to an identifiable individual.
- **Special Category Data:** Data relating to health, ethnicity, religion, biometric data, etc.
- **Processing:** Any operation performed on personal data.
- **Controller:** The organisation that determines how and why data is processed.
- **Processor:** A third party processing data on behalf of the controller.

For learner data funded by DfE or financed via Advanced Learner Loans, the Organisation acts as a **Data Controller**, and in some circumstances a **Joint Controller** with DfE or SLC where defined in contract.

4. Data Protection Principles

We comply with the UK GDPR principles:

1. Lawfulness, fairness and transparency
 2. Purpose limitation
 3. Data minimisation
 4. Accuracy
 5. Storage limitation
 6. Integrity and confidentiality
 7. Accountability
-

5. Lawful Bases for Processing

We process personal data under the following lawful bases:

- **Contract** – to deliver training and qualifications
 - **Legal obligation** – DfE funding rules, ILR returns, SLC reporting, audit
 - **Public task** – delivery of publicly funded education
 - **Legitimate interests** – business operations
 - **Consent** – marketing and optional services
 - **Substantial public interest** – safeguarding and equality monitoring
-

6. Data We Collect

Learners

- Identity and contact details
- National Insurance number
- Unique Learner Number (ULN)
- Loan information (via SLC processes)
- Prior attainment
- Attendance and achievement data
- Equality and diversity data
- Learning support needs
- Safeguarding information

Staff

- Employment records
 - Payroll and pension data
 - DBS information
 - Performance and disciplinary records
-

7. Sharing of Data

We share data where required with:

- Department for Education
- Student Loans Company
- Ofqual-recognised Awarding Organisations
- Ofsted
- HMRC (where required)
- Auditors and funding assurance bodies

Data is shared securely and only where lawful.

8. Advanced Learner Loans – Specific Provisions

In relation to Advanced Learner Loans:

- We collect and submit accurate learner data through the Individualised Learner Record (ILR).
 - We verify learner identity and eligibility in accordance with DfE funding rules.
 - We cooperate with SLC in confirming attendance and withdrawals.
 - We retain evidence required for funding assurance and audit.
 - We notify SLC promptly of learner status changes.
-

9. Transparency and Privacy Notices

We provide clear privacy notices explaining:

- What data we collect
- Why we collect it
- Who we share it with
- Retention periods
- Individual rights

Privacy notices are provided at enrolment and published on our website.

10. Data Subject Rights

Individuals have the right to:

- Access their data
- Rectification
- Erasure (where applicable)
- Restrict processing
- Data portability
- Object to processing
- Not be subject to automated decision-making

Requests must be responded to within one month.

11. Data Security

We implement appropriate technical and organisational measures including:

- Role-based access controls
- Multi-factor authentication (where available)
- Encrypted devices and secure cloud storage
- Secure password protocols
- Staff training
- Clear desk and screen policy
- Secure disposal of records

We comply with Cyber Essentials requirements where applicable.

12. Data Retention

Retention periods comply with:

- DfE Funding Rules (currently minimum 6 years after funding year end)
- SLC contractual requirements
- Awarding organisation requirements
- Statutory limitation periods

A separate Data Retention Schedule is maintained.

13. Data Breaches

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

We will:

1. Record all breaches
 2. Assess risk
 3. Notify the Information Commissioner's Office (ICO) within 72 hours where required
 4. Notify affected individuals where there is high risk
-

14. Data Protection Officer (DPO)

Where required under UK GDPR, we appoint a Data Protection Officer.

If not required to appoint a DPO, we designate a Data Protection Lead responsible for compliance.

Contact:

Neil Evans
neil@anydriver.co.uk
07827 228558

15. Data Protection Impact Assessments (DPIAs)

We conduct DPIAs where processing is likely to result in high risk, including:

- New MIS systems

- Monitoring technologies
-

16. Safeguarding and Special Category Data

We process safeguarding and special category data under:

- Substantial public interest
- Safeguarding of adults at risk

Access is strictly limited.

17. Marketing and Communications

Marketing communications are sent only:

- With consent (where required under PECR)
 - With opt-out options
 - In accordance with ICO guidance
-

18. International Transfers

We do not transfer data outside the UK

19. Staff Responsibilities

All staff must:

- Complete annual data protection training
- Follow this policy
- Report suspected breaches immediately
- Only access data necessary for their role

Failure to comply may result in disciplinary action.

20. Governance and Accountability

The Organisation maintains:

- Records of Processing Activities (ROPA)
 - Data sharing agreements
 - Processor contracts compliant with Article 28 UK GDPR
 - Audit trails
 - Annual policy review
-

21. Complaints

Individuals may complain to:

Information Commissioner's Office (ICO)

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

www.ico.org.uk

We encourage individuals to raise concerns with us first.

22. Policy Review

This policy will be reviewed annually or sooner where:

- Legislation changes
 - DfE or SLC requirements change
 - Following a serious data breach
-

Document Ref.	Title	Version	Date / Change	Reviewer	Next Review Date
ADP002	Data Protection Policy	1	November 19		November 2020
		2	January 2020	D Gardiner MBE	January 2021
		3	April 2021	D Gardiner MBE	April 2022
		4	January 2023	D Gardiner MBE	January 2024
		5	January 2024	D Gardiner MBE	January 2025
		6	February 2025	D Gardiner MBE	February 2026
		7	February 2026 / Full re-write to comply with new legislation.	D Gardiner MBE	February 2027

Policy Approved by: Neil Evans

Signature: N Evans