

Privacy Policy – Auctore Limited

Last updated: 01 January 2026

1. Introduction

Auctore Limited (“**Auctore**”, “**we**”, “**us**”, or “**our**”) is committed to protecting personal data and respecting privacy.

This Privacy Policy explains how we collect, use, disclose, and safeguard personal data when you:

- Visit our website
- Engage with our services
- Use our online cyber risk awareness training platform

This policy is provided in accordance with:

- The UK General Data Protection Regulation (“UK GDPR”)
 - The EU General Data Protection Regulation (“EU GDPR”)
 - The Data Protection Act 2018
-

2. About Us (Data Controller Details)

Data controller: Auctore Limited

Registered address:

Level 37, 1 Canada Square
Canary Wharf
London
E14 5AA
United Kingdom

Email contact: support@auctore.com

Auctore has not appointed a Data Protection Officer. Data protection matters are handled by our management and security team.

3. Whose Data We Process

We may process personal data relating to:

- Website visitors
 - Prospective customers
 - Customer administrators
 - Learners/end users accessing training on behalf of their employer
 - Individuals who contact us for support or enquiries
-

4. Controller and Processor Roles

4.1 When Auctore Acts as Data Controller

Auctore acts as **data controller** where we determine the purposes and means of processing, including:

- Website analytics and cookies
- Sales, marketing, and enquiry handling
- Account administration for customer contacts
- Compliance and security monitoring

4.2 When Auctore Acts as Data Processor

Where an organisation (such as an employer or corporate customer) provides learner data and determines how training is assigned or used, that organisation is the **data controller** and Auctore acts as a **data processor**.

In these circumstances:

- We process learner data only on documented customer instructions
 - Processing is governed by a Data Processing Agreement (DPA)
 - Learners should primarily direct rights requests to their employer, although we assist as required
-

5. Personal Data We Collect

5.1 Data You Provide Directly

- Name
- Business contact details (email, organisation)
- Job title or role
- Account login credentials
- Training progress, completion records, and assessment results

- Communications sent to us (support tickets, enquiries)

5.2 Data Provided by Our Customers (Art. 14 GDPR)

Where training access is provided by an employer or customer, we may receive:

- Name and business email address
- Organisation and department
- Assigned training records and completion status

This data is typically provided at account creation or enrolment.

5.3 Data Collected Automatically

When you visit our website:

- IP address
- Browser type and version
- Device and operating system information
- Pages visited and interaction data
- Approximate location derived from IP
- Referral source

This data is collected using cookies and similar technologies (see Section 11).

6. How and Why We Use Personal Data (Purposes)

We process personal data to:

- Provide and administer cyber risk awareness training
 - Create and manage user accounts
 - Track learner participation and completion
 - Communicate with customers and users
 - Respond to enquiries and support requests
 - Improve our website, platform, and services
 - Maintain platform security and prevent misuse
 - Comply with legal and regulatory obligations
-

7. Lawful Bases for Processing (Art. 13)

We rely on the following lawful bases:

- **Contractual necessity** – to deliver services under customer agreements

- **Legitimate interests** – for service operation, improvement, and security (balanced against user rights)
- **Legal obligation** – compliance with applicable laws
- **Consent** – where required (e.g. non-essential cookies, marketing)

Where consent is used, it may be withdrawn at any time.

8. Automated Decision-Making

Auctore does **not** use automated decision-making or profiling that produces legal or similarly significant effects on individuals.

9. Data Sharing and Recipients

We do not sell personal data.

We may share data with:

- Cloud hosting and infrastructure providers
- Analytics and monitoring providers
- Learning management or platform support services
- Professional advisers (legal, accounting, compliance)
- Regulatory or law enforcement bodies where legally required

All third parties are subject to contractual confidentiality and data protection obligations.

10. International Data Transfers

Some service providers may process data outside the UK or EEA.

Where this occurs, we ensure appropriate safeguards, including:

- UK adequacy regulations
 - EU adequacy decisions
 - Standard Contractual Clauses (SCCs)
 - UK International Data Transfer Agreements (IDTAs)
-

11. Cookies and Tracking Technologies (ICO-Aligned)

We use cookies and similar technologies to:

- Enable essential website functionality
- Analyse website usage
- Improve performance and user experience

11.1 Cookie Consent

In line with ICO guidance:

- Non-essential cookies are **not set without consent**
- Users are offered **equal options to accept or reject non-essential cookies**
- Preferences can be changed at any time via our cookie management tool

Further details are available in our Cookie Policy.

12. Data Retention

We retain personal data only for as long as necessary for its purpose.

12.1 Retention Schedule

Data Category	Retention Period
Website analytics	Up to 26 months
Marketing enquiries	Up to 24 months from last interaction
Customer contact details	Duration of contract + 6 years
Learner training records	Duration of contract + up to 6 years (customer-defined where applicable)
Support communications	Up to 24 months after closure
Security and access logs	6–12 months unless required for investigation

Retention may be extended where legally required.

13. Data Security

We apply appropriate technical and organisational measures aligned with recognised good practice, including:

- Role-based access controls

- Encryption where appropriate
- Secure hosting environments
- Monitoring and logging
- Incident management procedures
- Regular security reviews

No system is entirely secure, and absolute security cannot be guaranteed.

14. Your Data Protection Rights

You have the right to:

- Access your personal data
- Request correction of inaccurate data
- Request erasure (where applicable)
- Restrict processing
- Object to processing (including direct marketing at any time)
- Data portability
- Withdraw consent at any time
- Lodge a complaint with a supervisory authority

UK residents may contact the **Information Commissioner's Office (ICO)**.

Where Auctore acts as processor, requests should usually be directed to the relevant customer organisation.

15. Children

Our services are intended for business users. We do not knowingly collect personal data from children.

16. Changes to This Privacy Policy

We may update this Privacy Policy periodically. Changes will be published on this page with an updated "Last updated" date.

17. Contact Us

For privacy or data protection enquiries:

Email: support@auclore.com

Post:

Auclore Limited

Level 37, 1 Canada Square

Canary Wharf

London

E14 5AA

United Kingdom