
PRIVACY NOTICE

ASSESSABLE TECHNOLOGY LTD

1. Who we are

Assessable Technology Ltd (“Assessable”, “we”, “us”, “our”) provides an AI-enabled assessment and marking platform used by schools, academy trusts, and other educational organisations. This Privacy Policy explains how we collect, use, store, and protect personal data when you interact with us, our website, or our services.

Depending on how your data is used, we may act as either:

- a **data processor** (on behalf of a school or organisation); or
- a **data controller** (for specific activities including platform security, service improvement, and AI model training using pseudonymised data*).

**Academy Trusts/Schools/Parents are able to opt out of such data being used for AI model training. For more details please contact our Data Protection Officer using the contact details below.*

Contact details

Email: kate@cmlwconsulting.co.uk [Data Protection Officer](#)

Address: Office 57 South Tees Business Centre, Enterprise Court, Middlesbrough, United Kingdom, TS6 6TL

2. How this notice applies

This notice explains how we process personal data when:

- we do so for operational and marketing purposes
- learners’ work is submitted to our platform
- teachers and staff use our services
- data is used to improve and train our AI systems
- users interact with our website

Where your school uses Assessable, they remain the **primary data controller** for pupil and staff data used in marking and assessment.

3. Roles and responsibilities

3.1. When we act as a processor

We process personal data strictly under the documented instructions of the school or organisation.

3.2. When we act as a controller

We act as a data controller for:

- platform security and monitoring
- service improvement and analytics
- AI model training and evaluation using pseudonymised data
- Our own operational and marketing purposes

For these activities, Assessable determines the purposes and means of processing.

4. The data we process

4.1. **Processor activities (on behalf of schools)**

We process:

Pupil data

- Name or identifier (often minimised or pseudonymised)
- Submitted work (e.g. coursework, answers)
- Marks, grades, and feedback

Staff data

- Name, email address, role
- Account and usage data

4.2. **Controller activities (including training data)**

We process:

- operational data i.e. to manage our contractual relationship with a school as the supplier of the assessable platform.
- technical and usage logs
- system performance data
- pseudonymised assessment content and outputs used for model training and evaluation

This means:

- direct identifiers are removed or replaced
- data may still relate to an individual but cannot be identified without additional information
- additional information (e.g. key mapping identifiers) is kept separately and securely controlled

4.3. **Controller activities (website and marketing)**

We process:

Information you provide directly;

- Name
- Email address
- Telephone number
- Company name
- Billing and payment details

- Any information you submit via forms, emails, or correspondence

Information collected automatically

- IP address
- Browser type and version
- Device information
- Pages visited and interactions with our website
- Cookies and similar tracking technologies

Information from third parties

- Payment processors
- Analytics providers
- Business partners or referral sources (where applicable)

Our website may contain links to third-party websites. We are not responsible for their privacy practices or content.

5. How we use personal data

Processor purposes

- deliver AI-assisted marking
- generate feedback
- support moderation processes
- maintain system functionality

Controller purposes

- operational day to day management of our business
- ensure system security
- improve platform performance
- train and evaluate AI models using pseudonymised datasets
- reduce bias and improve accuracy

6. Lawful bases

The Assessable platform

Schools (controllers)

Typically rely on:

- public task
- legitimate interests (where appropriate)

Assessable (controller)

We rely on legitimate interests under [Article 6 UK GDPR](#) to:

- improve system accuracy and reliability
- enhance fairness and consistency
- maintain system security

We have conducted a Legitimate Interests Assessment to ensure:

- the processing is necessary
- impacts on individuals are minimised
- safeguards (including pseudonymisation) are effective

Other processing not related to the platform directly

- Contract – where processing is necessary to fulfil a contract with you
- Legitimate interests – for business operations and service improvements
- Legal obligation – to comply with applicable laws
- Consent – where you have explicitly agreed (e.g. marketing communications)

You may withdraw consent at any time.

7. AI and automated decision-making

Our platform uses AI to support marking and feedback.

- AI outputs are reviewed by teachers
- AI does not make final decisions
- human oversight is embedded

We do not carry out solely automated decision-making under [Article 22 UK GDPR](#).

8. AI governance and accountability

Assessable maps its operations so that it aligns with recognised standards such as;

- ISO/IEC 42001:2023 Information technology Artificial intelligence Management system
- ISO/IEC 23894:2023 Information technology Artificial intelligence Guidance on risk management
- ISO/IEC 22989:2022 Information technology Artificial intelligence Artificial intelligence concepts and terminology
- ISO/IEC 38507:2022 Information technology Governance of IT Governance implications of the use of artificial intelligence by organisations
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems
- ISO 9001:2015 Quality management systems

This includes:

- AI risk register
- lifecycle governance controls
- bias and fairness monitoring
- audit logging
- human oversight

9. Model training and pseudonymisation

Where data is used for AI training:

- identifiers are replaced or removed
- data is pseudonymised, not anonymised
- linkage keys are stored separately with strict access controls
- re-identification risk is assessed and minimised

This means:

- the data remains personal data under UK GDPR
- safeguards are applied in line with [Article 32 UK GDPR](#)

We do not use directly identifiable pupil data for model training.

10. Special category data

We do not intentionally process special category data.

If such data appears in submitted content:

- it is processed under school instructions
- additional safeguards apply

We do not infer sensitive characteristics.

11. Data sharing

We do not sell personal data.

We may share operational data with trusted service providers, subject to:

- contractual safeguards
- confidentiality obligations
- legal obligations
- security requirements

12. International transfers

Where data is transferred outside the UK:

- appropriate safeguards are used
- equivalent protections are ensured

13. Data retention (Processor)

Processor data: retained according to school instructions

14. Data retention (Controller)

AI Training Data Retention and Governance

- The Processor shall maintain documented governance controls relating to the retention, review, and disposal of datasets used for AI model development, testing, validation, monitoring, and improvement activities.
- Where pseudonymised Personal Data is used for AI-related purposes, the Processor shall ensure:
 - retention periods are defined, justified, documented, and periodically reviewed;
 - datasets are limited to the minimum necessary to achieve the legitimate and documented AI system purpose;
 - direct identifiers are removed or pseudonymised prior to use wherever feasible;
 - access is restricted to authorised personnel with appropriate role-based controls;
 - retained datasets are protected by appropriate technical and organisational security measures;
 - datasets are subject to bias monitoring, quality assurance, and governance oversight processes;
 - retention decisions are risk-assessed and documented as part of the organisation's AI governance framework; and
 - datasets are securely deleted, anonymised, or irreversibly de-identified once no longer required.
- The Processor shall maintain records sufficient to demonstrate accountability, governance oversight, and compliance with applicable AI governance and data protection obligations, including alignment with principles reflected within ISO/IEC 42001, ISO/IEC 23894, and associated AI risk management standards.

Data Category	Purpose	Example Retention Period	Notes
Customer operational data	Delivery of assessment services	As instructed by Controller	Deleted or returned on termination unless legally required
User account records	Account management and access control	Duration of contract + 12 months	Supports audit and dispute handling
System/security logs	Security monitoring and incident investigation	90 days	Longer retention where security incidents require
Authentication/access logs	Audit and access verification	6-12 months	Risk-based retention
Support tickets	Customer support and service improvement	24 months after closure	May contain limited personal data
Backups	Business continuity and disaster recovery	30-90 days rolling	Securely overwritten on rotation

AI training datasets (pseudonymised)	Model training and validation	Subject to periodic review, maximum defined internal retention period	Retention should be justified and documented
AI testing/validation datasets	Accuracy, bias and safety testing	12-24 months	Subject to governance review
Audit records	Compliance evidence	6 years	Depending on regulatory expectations
Deleted account suppression records	Prevent unintended re-creation / restoration	Limited minimal retention	Minimal data only
Financial/contractual records	Legal and accounting obligations	6 years	UK limitation and tax requirements
Incident investigation records	Security and compliance investigations	6 years or risk-based	May vary by severity
Cookies	Functional, statistics, marketing	Up to 1 year	User can manage consent via cookie settings tool

15. Security

We implement appropriate measures in line with [Article 32 UK GDPR](#), including:

- encryption
- access controls
- separation of identifiers and pseudonymised datasets
- monitoring and logging
- secure development practices

16. Cookies and similar technologies

We use cookies to ensure our website works effectively and to improve user experience. We manage cookie consent using [Complianz](#) GDPR Cookie Consent.

Users can:

- accept all cookies
- reject non-essential cookies
- customise preferences

A full list of cookies is available via the cookie settings tool on our website. To learn more about cookies visit <https://allaboutcookies.org/>

17. Your rights

You have rights under UK data protection law, including:

- access
- rectification
- erasure
- restriction
- objection

17.1. Exercising your rights

Where Assessable acts as a **processor**, requests should usually be directed to your school.

17.2. Exercising your rights with Assessable (controller activities)

Where Assessable acts as a **data controller** (including for pseudonymised training data), you may exercise your rights directly with us.

You can do this by contacting:

Email: kate@cmlwconsulting.co.uk – Data Protection Officer

When making a request, please:

- provide sufficient information to identify yourself
- specify the nature of your request
- include any relevant context (e.g. school attended)

17.3 Important clarification (pseudonymised data)

Because training data is pseudonymised:

- we may not be able to identify you directly from the dataset alone
- we may require additional information to locate your data
- in some cases, identification may not be possible without disproportionate effort

Where this applies, we will explain this clearly in our response.

17.4 Complaints

You have a right to complain. If you contact us using your preferred contact method from those stated in this privacy notice, we will address your complaint in line with our Complaints policy.

Should you feel we have not resolved your complaint you have the right to complain to the Information Commissioner's Office under [Article 77 UK GDPR](#).

18. Children's data

Our platform is designed for educational use.

We:

- process children's data under school instruction
- apply enhanced safeguards
- incorporate child-focused data protection principles

19. Updates to this notice

We may update this notice periodically.

The latest version will always be available on our website.

This privacy notice was last updated on 28/05/26.