Security statement

Last updated 21 August 2026

Security-conscious design

Nested Learning treats security as a design principle rather than a final technical check. We aim to reduce risk through proportionate safeguards, institutional oversight, secure development practices and continual improvement as the platform evolves.

Our AI tutor products are built to support learning, feedback, reflection, and evidence generation. Because these services may sit alongside institutional systems, we treat security as a design requirement rather than an afterthought.

This statement explains our current security approach in plain language. It does not disclose sensitive technical details, secrets, keys, infrastructure settings, or exploit-relevant information.

Our approach

Our approach is to reduce unnecessary risk through careful system design, proportionate technical and organisational controls, and regular review. We aim to minimise unnecessary access, limit the exposure of sensitive information, and support institutional confidence without collecting or retaining more information than is needed.

Access control

Access to the service is controlled through authenticated session mechanisms.

Learner sessions are scoped to the relevant organisation and to a pseudonymous user reference. This means that the system is designed to avoid relying on names or email addresses where a pseudonymous identifier is sufficient.

Access credentials are designed to be short-lived, limited in scope, and protected from browser exposure where possible. Long-lived or reusable access patterns are avoided where safer alternatives are available.

Administrative and diagnostic functions are protected separately from normal learner access. They require authenticated access and are not intended for public use.

Pseudonymisation and data minimisation

Nested Learning is designed to minimise the personal data needed to run an AI tutor session.

Where possible, the service uses pseudonymous session identifiers rather than direct personal identifiers. This supports safer session handling and reduces the amount of personal information processed by the AI tutor layer.

The system is intended to process only the information needed to provide the learning interaction, generate relevant feedback, and support agreed reporting or evidence functions.

Organisation-level separation

Session data is designed to be scoped to the authenticated organisation. This helps prevent one organisation's sessions, settings, rulebooks, or reports from being mixed with another organisation's data.

Where Nested Learning is integrated with a host institution or learning platform, the institutional configuration controls the relevant learning context. Nested Learning does not require unnecessary access to wider institutional systems.

Secure launch and integration controls

Where the AI tutor is launched from a learning platform, the launch process is designed to use short-lived, controlled access rather than permanent public links.

The system also restricts cross-origin access to approved origins. This means that browser-based access is not left open to any website by default.

The web bridge between a host site and the Nested Learning service is designed so that sensitive integration keys remain server-side and are not exposed to learners through the browser.

Safe rulebook and document handling

Nested Learning allows approved learning materials, rulebooks, or guidance documents to be used as part of tutor behaviour.

Document and rulebook ingestion is subject to safety controls. These include restrictions on file type, file size, and source handling. Temporary files are cleaned up after processing.

The system is designed to reject unsafe internal or private network targets when fetching rulebook material from URLs. This reduces the risk of server-side request forgery and related misconfiguration risks.

Secure development practices

Nested Learning is developed with secure coding practices in mind.

The backend uses structured data access patterns rather than relying on unsafe raw database queries. Dependencies are version-pinned to support more predictable builds and maintenance.

Secrets are supplied through protected environment configuration and are not intended to be committed to the code repository.

Security-related behaviours are tested where appropriate, including regression testing for protected administrative access.

Voice and text-to-speech security

Where voice or text-to-speech features are enabled, requests are designed to use controlled, time-limited access.

Voice and text features are optional parts of the learner experience and are handled through the same general principles of access control, session scoping, and data minimisation.

Monitoring, logging, and diagnostics

Nested Learning includes operational logging and diagnostic functions to support maintenance, troubleshooting, and security review.

Diagnostic tools are not intended for public access. They are protected separately and used to support safe operation, configuration checks, and issue investigation.

Logs are designed to support operational visibility without unnecessarily exposing sensitive learner information.

Current assurance position

Nested Learning is actively designed with cyber security good practice in mind.

We are on a journey towards Cyber Essentials certification, ISO 27001 certification, SOC 2 certification, or equivalent formal security accreditation, and this is a work in progress.

This statement should therefore be read as a transparent description of our current security approach, not as a formal certification claim.

Security assurance

We maintain supporting security documentation describing our security approach, governance arrangements and technical controls. More detailed assurance information may be made available to customers as part of procurement, due diligence or institutional security review.

Continuous improvement

Nested Learning is an evolving product. Security controls will continue to be reviewed as the platform develops, as pilots expand, and as institutional requirements become clearer.

Where a partner organisation has specific security, data protection, procurement, or technical assurance requirements, these should be reviewed through the appropriate institutional process before deployment.

Contact

Security or cyber security questions about Nested Learning can be raised through the contact routes provided on this website.

We welcome responsible disclosure of security concerns and will review reported issues in good faith.

Security Principles at-a-glance

Security principle	Nested Learning's current approach
Secure by design	Security considerations are incorporated throughout product design and development rather than added retrospectively.
Least privilege	We aim to minimise access, reduce unnecessary permissions and separate administrative functions from learner interactions.
Defence in depth	Technical and organisational safeguards work together to reduce risk and support institutional confidence.
Data minimisation	We seek to limit the personal data processed and reduce reliance on directly identifying information where possible.
Continual improvement	Security controls are reviewed and strengthened as the platform, customer requirements and threat landscape evolve.