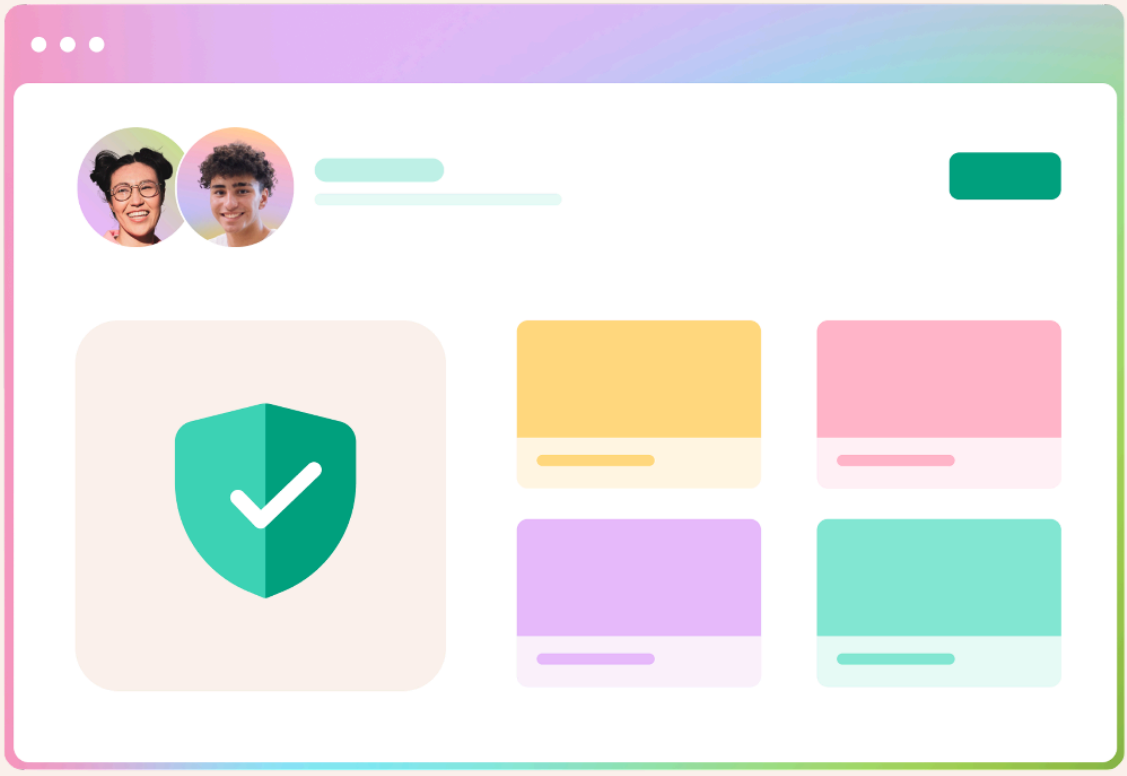
GrowHall

Privacy & Security Pack

How GrowHall protects your data

Last Updated: July 27, 2026



This pack describes the current state of GrowHall's security and AI practices, which are subject to change with future enhancements and product launches. This document is for informational purposes only and does not constitute legal advice, nor should it be interpreted as supplementing or being incorporated into any terms and conditions of any contractual agreements.

“

At Toddle, protecting student data has never been a feature we added. It's how we've built from the start, and it's why schools in over 100 countries trust us with their students' work.

When GrowHall became part of Toddle, **that same standard became the standard for GrowHall too**. It now runs on the same infrastructure and the same protections that safeguard every student on Toddle. Nothing less, because the students using GrowHall deserve exactly what every student on Toddle already has.

Deepanshu Arora, School Leader, CEO at Toddle

01

Introduction

GrowHall is a cloud-based learning-support platform that provides educational content, learning resources, assessments, and AI-assisted learning tools for schools, educators, and students (the "Service"). The Service is operated by Teacher Tools Private Limited ("we", "us", or "our"), the same company that operates **Toddle**.

GrowHall and Toddle share the same legal entity, the same hosting and security infrastructure, the same information security management system, and the same data protection programme. This pack sets out the measures, practices, and technologies that form the foundation of GrowHall's security and AI strategy.

Where a school uses GrowHall, the school is the data controller and Teacher Tools Private Limited is the data processor. The school decides what data is shared with the Service and the purposes for which it is used. We process that data only to provide the Service, to meet legal obligations, or on the school's documented instructions. **We do not sell personal data and do not use it for advertising.**

Useful Links

Terms of Service	:	https://www.growhall.com/terms-of-service
Terms of Use	:	https://www.growhall.com/terms-of-use
Privacy Policy	:	https://www.growhall.com/privacy-policy
Cookie Policy	:	https://www.growhall.com/cookie-policy
Sub-Processor List	:	https://www.growhall.com/3rdparty
Trust Vault	:	https://trust.toddleapp.com

02 Infrastructure

Hosting Provider

GrowHall is built on **Amazon Web Services** (SOC 1, SOC 2, and SOC 3 certified). To deliver the Service, GrowHall uses three main types of servers on AWS:

- **Storage servers**: where media such as documents, images, and video are stored. All files are encrypted at rest and in transit. GrowHall uses AWS S3 for this purpose.
- **Database servers**: a relational database storing data in organised tables, encrypted in transit and at rest.
- **Compute servers**: these handle user requests so the Service stays responsive.

Datacenter Locations

GrowHall offers AWS data center locations to customers who require their data to be stored in a specific region:

Region	Primary Data Center	Backup Location
Australia	Sydney	Melbourne
Europe	Ireland	Frankfurt
Hong Kong	Hong Kong	Hong Kong
Singapore	Singapore	Tokyo
United Arab Emirates	Dubai	Bahrain
United States of America	N. Virginia	Oregon

For users in other regions, data can be stored in any of the available locations.

Access to production

Access to GrowHall's production environment is strictly controlled and granted only on a need-to-know basis, following the principle of least privilege. Administrative privileges are reserved for a specialised team of engineers within the Infrastructure Team, with enforced password policies and mandatory Multi-Factor Authentication (MFA).

Encryption and key management

- **Encryption in transit.** All data in transit is protected by **TLS 1.2+** with strong ciphers, enforced for all connections including web, API, and email access.
- **Encryption at rest.** Data at rest is encrypted using **AES-256**. Encryption keys are managed through AWS Key Management Service (KMS).

Tenant Separation

The platform serves multiple customers with strict logical boundaries that keep each customer's data separate. This is achieved through a unique identification system that assigns a combination of parameters to create unique IDs, giving data segregation at the application level.

Service Level Commitment

GrowHall is committed to providing a reliable and secure service to its users. Service Level Commitment includes a server uptime guarantee of **99.9%**.

Separate Production Environment

GrowHall's development and testing environments are separate from production. Customer data is never stored in non-production environments.

Virtual Private Cloud

GrowHall uses AWS Virtual Private Cloud so that compute runs in a secured environment, separate from other public cloud tenants.

Backups

GrowHall takes continuous backups of user data using automated schedulers. Backups are held in a separate server location and encrypted using AES-256.

Data Type	Backup Type	Frequency
Database (AWS)	Incremental	Every 5 minutes (automated)
Database (AWS)	Full	Daily and monthly (automated)

03

Application Security

Design Reviews

The security team integrates security reviews into the product roadmap, ensuring that every major release undergoes threat modeling and design reviews to provide a secure experience for users.

Secure Deployment

As part of the software development lifecycle, any new feature is analysed for code quality and potential security vulnerabilities. Each feature passes a review process, including peer evaluation, before release.

Change Management

The change management process follows a formal policy maintained by the Engineering team. System modifications are tested and authorised before they reach production. Developers initiate source code changes, which are held in version control and must pass automated QA testing against security standards. Only after successful QA are changes deployed, with logs maintained and alerts sent to engineering management. Infrastructure changes are restricted to authorised personnel, with the security team overseeing infrastructure security, keeping servers up to date, and holding configurations to industry standards.

Web Application Firewall (WAF)

GrowHall uses AWS WAF to protect the platform from common web exploits.

Vulnerability and Penetration Tests

On an annual basis, a professional security assessment firm assesses GrowHall's web application to identify weaknesses. As part of the Information Security Management System (ISMS), findings and recommendations are reported to management, reviewed, and actioned. High-severity issues are documented, tracked, and resolved by dedicated security engineers.

Rate Limiting

Rate limiting restricts the frequency of requests from a user or IP address within a defined timeframe, mitigating denial-of-service attacks, brute-force attempts, and API abuse. Limits are calibrated to balance security and user experience, and are monitored and adapted to address evolving threats and usage patterns.

04

Operational Security

Information Security

We maintain a formal information security management programme with a dedicated team of security specialists reporting to the Chief Information Security Officer. The team implements and maintains security controls and monitors systems for potential threats.

Human Resources

> ***Hire right, set the expectations from the beginning, train well, review from time to time, and close the loop at the exit.***

Background checks. All personnel undergo background checks, following industry practice and applicable law.

Employment terms. Every employment contract includes confidentiality clauses and provisions for immediate termination in cases of specific breaches. An HR security policy sets out security responsibilities across an employee's tenure.

Acceptable use. An acceptable use policy is reviewed annually. Employees acknowledge it on joining and whenever it changes materially.

Training programme. All personnel complete information security training during onboarding, based on the Privacy Skill Matrix. Topics include data protection, phishing awareness, password hygiene, and incident response. Monthly security and privacy tips and annual refresher sessions keep these topics current.

Termination. On exit, all access is revoked within one business day.

User Access Reviews and Policy

GrowHall is proactive in managing access to its systems. Every month, the management team reviews user access to ensure it remains appropriate and removes any access that is no longer needed.

Data Center Security

GrowHall leverages AWS's robust physical and environmental controls, which are implemented in state-of-the-art facilities independently assessed through third-party audits, including SOC 1, SOC 2, and ISO 27001 certifications. Amazon consistently manages risk and undergoes regular evaluations to maintain compliance with industry-leading standards. For further details on their security practices, please visit **AWS Security Compliance**.

Governance and Risk Management

A dedicated Governance, Risk, and Compliance (GRC) team, supported by a GRC platform, manages the ongoing risk assessment process. The team identifies vulnerabilities, evaluates emerging threats, reviews policies and procedures against industry standards, determines the controls needed, conducts internal audits, and facilitates independent third-party audits. This is the same GRC function that operates for Toddle.

Monitoring and Logs

GrowHall uses Amazon Cloud Watch and CloudTrail, with custom scripts that extract log data into monitoring services. We monitor capacity utilisation of physical and computing infrastructure against service levels. AWS GuardDuty continuously monitors for malicious or unauthorised behaviour, including unusual API calls, potentially compromised instances, and unauthorised access attempts, with alerts integrated into security workflows. Application and server logs are retained in CloudWatch for 3 years; other machine monitoring logs for one week.

Data Retention and Disposal

Data retention. We retain your information for the duration of the contract term. After contract termination or expiry, information is retained for up to seven years, or for as long as necessary to fulfil the purposes set out in the Privacy Policy, subject to applicable law or the customer's documented instructions, whichever period is shorter. Data processed on behalf of customers is retained under the Terms of Service, the Data Processing Agreement, applicable law, and any other relevant agreement.

Data deletion. You have the right to erasure. To delete a GrowHall account or content, contact privacy@growhall.com. We notify you by email before deletion. After a request, we may retain information for up to 365 days to provide support and prevent accidental deletion. A Data Deletion Certificate is available on request and can be used as evidence during audits.

For users in the USA, to comply with FERPA, GrowHall may need to retain certain student education records once a valid request to inspect those records has been made.

Data destruction. GrowHall hosts on AWS. AWS applies data distribution and deletion strategies for multi-tenant environments, and follows NIST 800-88 techniques when storage media is decommissioned.

Incident Response and Management

The incident response framework includes policies and procedures to address issues of service availability, data integrity, security, privacy, and confidentiality. Specialised teams are prepared to:

- **Immediate Response:** Quickly react to alerts signaling potential incidents.
- **Incident Assessment:** Evaluate the severity and scope of the incident.
- **Mitigation & Containment:** If required, initiate appropriate measures to mitigate and contain the impact.
- **Evidence Collection:** Secure and preserve any evidence for further investigation.
- **Post-Incident Analysis:** Document the findings, create a postmortem report, and develop long-term strategies to prevent recurrence.

Notification. Where GrowHall acts as processor, we notify the affected school (as controller) as soon as possible after becoming aware of an incident, with a description of the incident, the categories of data involved, and the steps taken. The school, as controller, handles onward notification to regulators or data subjects, with our support, in line with the timelines that apply to it. Indicative regulator timelines by country are below.

Indicative regulator notification timelines by country

Country	Notification Timeline	Law / Regulation
Australia	Within 30 days of becoming aware	Notifiable Data Breaches (NDB) scheme
Brazil	Within a reasonable time	LGPD
Canada	As soon as feasible	PIPEDA
European Union	Within 72 hours	GDPR
Hong Kong	As soon as practicable	PDPO
India	Within 6 hours of noticing the incident	CERT-In Rules 2013
Saudi Arabia	Without undue delay	PDPL
Singapore	As soon as practicable, no later than 3 days	PDPA
South Korea	Within 24 hours	PIPA
Switzerland	As soon as possible	FADP
Turkey	Without undue delay	KVKK
UAE	Without undue delay	Federal Decree-Law No. 45 of 2021
United Kingdom	Within 72 hours	DPA 2018 / UK GDPR
United States	Varies by state, generally 30-60 days	State breach notification laws
All other countries	As soon as reasonably possible, per local regulation	Local data protection laws

Disaster Recovery and Business Continuity

The Business Continuity Plan is designed to handle disruptions and restore critical systems quickly. Using AWS disaster recovery tooling, GrowHall targets a Recovery Time Objective (RTO) of **3 hours** and a Recovery Point Objective (RPO) of **5 minutes**. During such events, service levels and turnaround times are temporarily paused and the Business Continuity Team oversees the response. The plan is tested annually, with results shared with customers.

Third-Party Service Providers

We partner only with third-party service providers whose security measures align with our policies.
Before any vendor is used, the GRC team reviews the vendor's security protocols, data retention and privacy policies, and security track record. All providers sign a written agreement with data protection obligations at least as strong as our own technical and organisational measures. Critical vendors are reevaluated annually.

GrowHall's current sub-processor list is available at https://www.growhall.com/3rdparty.

05
IT Security

Endpoint Security

All endpoints run the latest OS version and a centrally managed Endpoint Detection and Response solution with Extended Detection and Response capabilities (SentinelOne), monitored by a 24/7 Security Operations Center. Devices use FileVault or BitLocker encryption, password protection, and automatic screen timeouts. An enterprise Mobile Device Management solution (Scalefusion) allows remote patching and device wipe.

Password Protection

Password guidelines for all personnel:

- At least 8 characters
- Changed every 60 days
- No common passwords (such as "reset" or "admin")
- Not shared with anyone, and account access not given to others
- At least one numeral, one special character, and one letter
- Not the same as the user name
- No personal information (such as date of birth or name)
- Not revealed by phone or email
- Not written down or stored anywhere

Email Protection

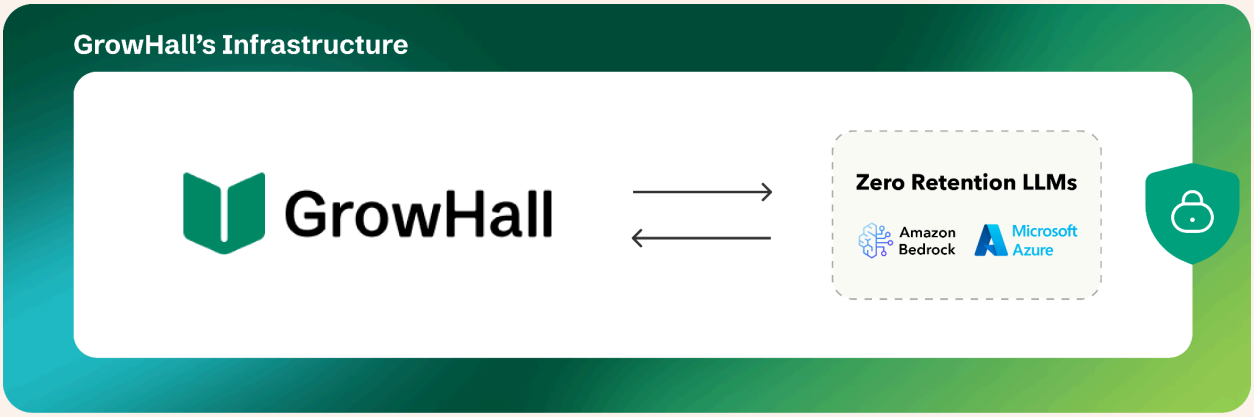
We use Google Workspace as the email provider, with DMARC and SPF in place. We provide ongoing training to all employees on how to identify and avoid phishing attempts, and regularly test their knowledge to ensure they're prepared for real-world scenarios.

06

Data Privacy with GrowHall AI

Responsible Model Deployment Strategy

Our AI features are deployed within GrowHall's own cloud accounts, which form our trust boundary for AI processing. The models we use are hosted there as managed services, under written contracts with each provider. This means your prompt data is processed inside that boundary and is not sent to the model developers' own services.



Our current model providers, also listed in the sub-processor list, are:

- **Amazon Bedrock (Amazon Web Services, Inc.),** used to access Anthropic's Claude models within our own AWS account.
- **Microsoft Azure OpenAI Service (Microsoft Corporation),** used to access OpenAI's models within our own Azure tenant.

By regionally hosting these models within the **United States**, **Europe**, and **Australia**, we ensure our customers' data remains within its designated region. This allows us to maintain strict control over data residency, comply with local regulations, and securely manage all AI use cases end-to-end.

We do not use any user-generated data to train or develop language models or similar AI systems. User-generated data is processed solely to provide the Service, in line with the Privacy Policy. We evaluate models for accuracy, hallucination rate, and latency.

AI Development Principles

01 **Purpose-driven design.** We build AI features to address real classroom and learning needs, not to replace professional judgment. If a feature does not make teaching or learning simpler or more meaningful, we do not build it.

02 **Privacy and security from the ground up.** We treat student and educator data with care, applying encryption, access controls, and review across the AI development lifecycle. Data is used only to deliver the Service.

03 **Ethical and sustainable innovation.** We assess our AI features for negative effects, including on student wellbeing, and make improvements.

04 **Bias awareness and fairness.** We work to identify and address bias in AI outputs, refining our approach and adding safeguards where needed.

05 **Human oversight and accountability.** Educators remain in control. AI suggestions are suggestions. The educator decides what to use.

06 **Transparent and user-centric.** Every AI feature is clearly labelled, so users know when they are interacting with AI.

07 **Global compliance and ongoing improvement.** We align AI development with the EU AI Act, ISO 42001, GDPR, COPPA, FERPA, and other applicable frameworks, and refine our approach as guidance evolves.

AI Security and Safety Measures

Security testing

- Penetration and jailbreak testing of AI security controls.
- Automated vulnerability scanning of AI integrations.
- Access control checks confirming only authorised users reach AI features and that permissions are enforced.

Safety testing

- Bias and fairness analysis of AI outputs.
- Explainability verification, testing whether responses are clear and interpretable.
- Edge case validation under rare or unpredictable scenarios.
- Content and interaction integrity checks.
- Monitoring for and blocking of harmful, misleading, or inappropriate outputs.

07

Privacy Policy and Compliance

Privacy Policy

GrowHall's Privacy Policy details its current data practices and is regularly updated to reflect any changes. This document outlines the information GrowHall collects and processes, as well as how individuals can exercise their privacy rights under applicable laws.

- We collect personal information such as name, email, and usage data for account creation and to provide the Service.
- The school determines what data is shared and the purposes for which it is used.
- We do not share data for advertising and do not sell data.
- We never sell data to anyone for any purpose.
- Users can access, correct, update, or delete their data and restrict certain processing, exercised through the school as controller.
- Cookies are used to support the user experience.
- Data is retained as long as needed for the stated purposes or as required by law.
- We comply with GDPR, COPPA, FERPA, CCPA, DPDPA, APPs, PDPL, and other privacy laws.
- Cross-border transfers are protected to applicable standards.
- Users are notified of significant Privacy Policy changes.

Compliance with Global Privacy Laws

GrowHall is built to support schools in meeting their obligations under the data protection laws that apply to them. The school remains the controller and holds the legal basis for processing. We process as instructed and provide the documentation and controls schools need.

GDPR (EU/EEA and Switzerland)

We offer a Data Processing Agreement to EU/EEA and Swiss customers, signed at onboarding. Processing is lawful, purpose-limited, and minimised, and data is encrypted in transit and at rest. When a school uses GrowHall, the school determines the lawful basis for processing and obtains any notices or authorisations required under applicable law. We act as processor on the school's documented instructions and do not determine the lawful basis. Data subject rights (access, rectification, erasure, portability) are supported, with portability provided in a machine-readable format.

FERPA (USA)

Student records provided by an educational institution remain the property of and under the control of that institution. We use student record information only for purposes permitted by the Terms of Use and Privacy Policy, limit employee access, conduct background checks and training, and notify the institution in the event of an unauthorised disclosure. We do not use student records for targeted advertising.

COPPA (USA)

As a third-party operator, we rely on school consent for children under COPPA and operate as a School Official under FERPA for children under 13. Student accounts are created by teachers, and content visibility is controlled by the school.

CCPA (USA)

As a service provider, we support the California Consumer Privacy Act: the right to know, delete, opt out of sale (we do not sell personal information), non-discrimination, limit, and correct. We process personal information only on the school's documented instructions and do not share it for cross-context behavioural advertising.

DPDPA (India)

We are committed to the Digital Personal Data Protection Act, 2023. As a Data Processor, we process data on the instructions of the Data Fiduciary (the school), who is responsible for obtaining verifiable parental consent before sharing a child's personal data. We apply security measures and support data principal rights, including access, correction, erasure, grievance redressal, and nomination.

Thank you for trusting us!

GrowHall