Stile

Security and Privacy Guide

For School Leaders and ICT Executives



Need help?
Contact **1300 918 292** to talk to our Melbourne-based team.

Urgent security or privacy matter?
Contact a Stile engineer 24/7 on **+61 3 4829 5555** for critical emergencies

Version 1.6

The Platform of Choice

We know that choosing a technology platform for students and teachers is hard. The endless parade of minimum-viable startups offering exciting new products on a shoestring budget are a constant temptation, while the industry giants have experience and expertise, but only a passing interest in delivering good learning experiences en route to conquering another industry vertical.

Stile offers a third way: as a **for-purpose company** with more than a decade of experience providing the world's best science lessons to **more than 1000 schools**, our **Melbourne-based team** has the experience, expertise and impetus to deliver a secure, stable responsibly managed platform, combined with a singular focus on providing the best possible science education for every student, and **respecting their privacy in the process.**

Stile was co-founded in 2012 by Dr. Alan Finkel (Australia's chief scientist from 2016 to 2020 and an incurable engineer) for one purpose: to improve the quality of science education. Stile's core leadership team of scientists, teachers and engineers has been with the company since those early days and drive a comprehensive culture of quality that infects every aspect of our operations: from the beautiful physical books your teachers receive at the start of each year; to the deeply considered, rigorously tested pedagogies embedded in every lesson; and the impeccable engineering that delivers those lessons on the most **stable, secure, and effective platform available today**.

Throughout this document, you will find ample evidence of Stile's dedication to providing the best possible teaching platform, and our relentless commitment to continuously improving education technology.

Stile is for schools that are serious about science. Serious about challenging their students and supporting their teachers. Serious about keeping them safe, and secure.





Daniel Rodgers-Pryor
Chief Technology and Security Officer
With Stile Education since 2014

Table of Contents

The Platform of Choice 2

What is Stile? 4

Our Security and Privacy Principles 5

Purpose driven 5

Private by default 5

Always secure 5

Australian Privacy Principles 6

Data Breach Notifications 6

Secure Data Storage 6

Data We Collect 7

External Assessment 9

Safer Technology for Schools (ST4S) 9

Human Rights Watch 9

Student Privacy Pledge 9

Penetration Testing 10

Open Bug Bounty 10

System and Organization Controls (SOC2) 11

Data Processors 12

Data Storage & Processing 12

Transient Data Processing 13

Stile's Architecture 14

Network Security 14

Incident Response 16

What happens when there's a problem? 16

Staff Access 17

Stile Staff Security 18

Frequently Asked Questions 19

How does Stile manage changes to its systems? 19

Does Stile encrypt all data at rest and in transit? 21

How does Stile protect passwords? 21

How does Stile secure session tokens? 22

How does Stile protect against Cross Site Scripting (XSS) Cross Site Script inclusion (XSSI) attacks? 22

How does Stile protect against Clickjacking attacks? 23

How does Stile protect against SQL Injection attacks? 23

How does Stile protect against Server Side Request Forgery (SSRF) attacks? 23

How does Stile secure user uploaded files? 24

Is all software kept up-to-date? 24

How are Stile's servers hardened against vulnerabilities? 25

How are staff devices secured? 25

How is our data backed-up? 26

Does Stile keep logs of activity in its systems? 26

What is Stile?

Stile is the best way to teach science. Stile is the core curriculum resource for your science department. Lesson plans, videos, workbooks, assessments, rigorous teaching notes, simulations, real-time analytics, professional learning and more. All beautifully crafted to work seamlessly together. Every week, more than 250,000 students and their teachers depend on Stile to explore important global issues and the latest scientific discoveries in their classrooms.

Our robust online platform (**stileapp.com**) allows teachers to pull-in world-class lessons and edit every detail of them to suit their students' unique needs. During class, students answer carefully crafted questions in the context of real-world science discoveries and events, helping spark conversation and debate. Without breaking stride, teachers can track student progress in real time throughout a lesson, direct their time where it's most needed, and deliver effective feedback.

Crafted with care by our science and engineering teams in Melbourne, and hosted by Amazon Web Services in Sydney and Oregon, Stile's battle-hardened platform allows you to get started without installing or configuring anything. We've always prioritised keeping Stile updated, secure and safe by default, so that you don't need to worry.

Stile Education is a privately owned and operated Australian company. Our headquarters is located on the traditional lands of the Boon Wurrung and Woiwurrung (Wurundjeri) peoples of the Kulin Nation. We acknowledge that sovereignty was never ceded and pay our respects to Elders past, present and future.



Our Security and Privacy Principles

Purpose driven

Stile's core goal is always to provide the best possible science education for every student: we're not here to gather data about you, or sell you unrelated products and services.

Stile is the product, you are not.

Stile only collects your data in order to provide our ever-improving educational services to you. We do not claim any ownership over your data: it's yours, not ours. We do not and will never use your data to advertise or sell/give your data to third parties.

Private by default

Every student and teacher using Stile has their own account that only they can access, and those accounts only gain access to lessons and other content when explicitly allowed by an administrator, teacher, or central single sign-on identity provider system. For every lesson a teacher creates and every piece of work a student submits, we manage a robust set of security rules that specify exactly who can view and modify them; there's nothing you need to configure, your data is already safe. All data sharing between users (eg. sharing responses to a live brainstorming session) requires explicit opt-in and moderation from the class teacher.

Always secure

We aren't satisfied with a technology industry that leaks millions of customer records each month, and you shouldn't be either. Stile looks across the world wide technology landscape to draw on the best available practices, and frequently pushes the boundaries when current best solutions aren't good enough.

We've built Stile from the ground up with the privacy and security requirements of schools and students in mind. Stile's development processes ensure that security is a core consideration whenever we add new features or modify existing ones. We use automated systems to randomly audit our security policies, ensuring they are correctly enforced. Internal and third party reviews of our security practices are routinely performed to verify our security practices and identify potential vulnerabilities.

To provide you with helpful and timely support, a strictly limited number of our highly trained staff have access to your data on an as-needed basis and only when you have explicitly given us permission. All staff access is centrally provisioned through minimum-privilege role based access control. All access by staff and automated systems is comprehensively and immutably logged, and those logs are regularly audited.

All staff at Stile are required to hold a valid **Australian Working with Children** check. We work with all of our employees to ensure that they adhere to best-practice personal security guidelines that cover device security, encrypted file storage, password policies, social engineering and more.

As a small company, we know our limits: Stile is hosted with Amazon Web Services (AWS), who are the world's preeminent experts at providing reliable and secure server infrastructure. AWS is responsible for the physical security of the infrastructure that runs Stile. Amazon's global reach allows us to seamlessly host Australian data in Sydney, and US data in Oregon, guaranteeing data sovereignty, and low latency.

Thanks to our ongoing diligence, **Stile has never suffered a data breach.**

Australian Privacy Principles

Stile fully embraces and extends upon the **Australian Privacy Principles**. In particular, Stile strives to collect the **minimum** amount of information about you that we need in order to provide our services, define new stronger industry standards for **securing** that information, and **never selling** or giving your information to third parties, and **never** using it for **advertising**.

Secure Data Storage

All data, including backups are securely stored in Australia. All data is stored and processed with Amazon Web Services (AWS), the world's leading cloud services provider. AWS provides **exceptional physical security** for all data that they handle, and multiple layers of encryption and network security prevent any unauthorised access.

Data Breach Notifications

If data that Stile holds about you is ever compromised, or if we suspect that it has been compromised, Stile will notify you. Notifications will generally come via your school, district, diocese or state government as appropriate.

Stile aims to fully contain and mitigate all security breaches within 24 hours of discovery, and then notify affected people and organisations immediately afterwards. Initial notification of a security breach will never take more than **7 days from the time of discovery.**

In addition to contacting you directly, Stile will report breaches to the Office of the Australian Information Commissioner, US State Attorneys General, and all other relevant authorities.

Stile's Data Breach Response Policy is fully compliant with the Australian government's **Notifiable Data Breach Scheme**.



Data We Collect

Stile takes care to only collect data that's strictly necessary for providing fantastic services to our teachers and students. Stile fully supports pseudonymous usage, and allows teachers to see, limit and moderate all student data.

No **sensitive** data (eg. health records, criminal records, sexual preferences etc.) is collected by Stile, but Stile does allow for rich textual responses from students with moderation from teachers to ensure that only appropriate information is provided. Stile protects all collected data with industry leading security and privacy practices which are appropriate for handling both sensitive and private data.

Type of Data	Required?	Comments
Student Names	Optional	Stile displays student names (or optionally pseudonyms) to teachers when marking student assessments, arranging classes, and to enable moderation of class discussions, polls etc. If Single Sign On (SSO) is not used, then students are presented with the option to enter a name when they first sign up to the platform. If SSO is used, then student names are set automatically based on data sent from the school's identity provider system.
Student Emails	Optional	Stile allows students to recover their passwords via email (if not using SSO) and notifies them when teachers invite them to new classes. Students can optionally use anonymous email addresses created by their school.
Teacher Names	Optional	Teachers can enter a name (or pseudonym) to be shown to their students in the platform, and an alternate name (or pseudonym) that will be presented to their colleagues in the platform.
Teacher Emails	**Required**	Teacher email addresses are used for invitations, password recovery and transactional communications about their classes. Teachers are asked for their email when signing-up (if not using SSO)
Teacher media uploads	Optional	Teachers can upload files for their students including videos, photos documents and other media as part of building a lesson in the Stile platform
Student media uploads	Optional	Teachers can optionally request that students upload their work as a file, including photo/video files. If a teacher has enabled a moderated class discussion, then students can upload files to the discussion, including photos. Students can't upload files, photos, videos or other media unless a teacher has enabled one of the above features.

Type of Data	Required?	Comments
Attendance record data	Optional	Stile allows teachers to optionally select 'absent' as the reason for a student's assignment being incomplete, but Stile does not support maintaining a comprehensive attendance record.
Student work	**Required**	Students in Stile complete worksheets, including free text questions, multiple choice questions, interactive simulations and other kinds of student work.
Student results	**Required**	Student work on assessments in the Stile platform is marked (automatically for some kinds of questions, or manually by the teacher for others) and those marks are tabulated and displayed to teachers in the platform. Qualitative feedback from teachers is also collected.
Student chat comments	Optional	Stile allows optional in-class discussion, if the feature is enabled and moderated by a teacher. Stile also allows students to collaboratively brainstorm solutions to problems, and these submissions can optionally be shared within the class by a teacher.
Passwords	Optional	If using a SSO integration, Stile does not collect or allow the use of passwords. Otherwise, all users (teachers and students) are identified by a password stored by Stile using a modern, secure password-hashing algorithm (bcrypt).
Usage metadata	**Required**	Stile automatically records usage of the platform and actions taken in the platform. This data is used for multiple purposes: providing the core platform services (eg. showing authorship of a response in the platform), for security and audit purposes (allowing our support team to track down unexpected changes), to enable effective operation of Stile's infrastructure (eg. predicting numbers of running classes so that servers can be provisioned), and to inform the development of improvements to the product (eg. monitoring anonymised usage of a new kind of question).
Browser IP addresses & User Agent	**Required**	Stile collects user agent strings and IP addresses from all requests automatically for security purposes, so that users can see where their account has been used from.

External Assessment

We're always seeking external review and criticism to help us improve. Don't just take our word for it: see how we compare to industry benchmarks.

Safer Technology for Schools (ST4S)

The **ST4S** program is a national initiative to provide a common benchmark for assessing privacy and security practices and measuring risk levels from the use of technology in schools. Stile worked with the ST4S team during the initial development of the program in 2019 and we remain enthusiastic proponents of stronger privacy and security standards in the education sector. **Stile has an ST4S Badge** and consistently achieves the best possible safety ratings. Stile performs annual ST4S Readiness Checks to ensure that our certification remains current.

How to See Stile's ST4S Report

Under the terms of the ST4S program, we can't directly provide you with a copy of our assessment report, but you can request it by contacting your state education department below.



Independent Schools

Independent Schools Australia: **st4s@isa.edu.au**

Public schools

VIC: **infosafe@education.vic.gov.au**

NSW: **information.security@det.nsw.edu.au**

QLD: **riskreviews@qed.qld.gov.au**

WA: **privacy@education.wa.edu.au**

SA: **education.ictcybersecurity@sa.gov.au**

TAS: **security@education.tas.gov.au**

NT: **cloudsystems.doe@ntschools.net**

Human Rights Watch

As a result of Stile's ongoing commitment to privacy and security, a **2022 Human Rights Watch report** found Stile to be one of only 12 (out of 124) education technology companies handling student data appropriately.

> *"HRW said five of the 12 companies analysed in this way were "clean" and able to operate without privacy concerns, including a product used in Australia called Stile Education."*
> – From the **ABC's coverage of the HRW report**.

> *"The Human Rights Watch study identified nine apps that they say seemed to protect their users' data and privacy around the world. They include Stile Education"*
> – From the **Washington Post's coverage of the HRW report.**

Student Privacy Pledge

The **Student Privacy Pledge** is a program run by the **Future of Privacy Forum (FPF)** and the **Software & Information Industry Association (SIIA)** to set a standard for education technology providers around the world. Stile **passed the assessment process**, and is fully committed to the pledge as part of our long standing commitment to impeccable privacy and security.



Penetration Testing

At least once a year, Stile hires expert hackers to try and break into our production systems and find vulnerabilities or design flaws that we may have missed. The exact targets (public APIs, back of house systems etc.) vary each time based on our assessment of the evolving threat landscape, but we always make sure that these are *open-book tests*, **where the attackers have full access to Stile's source code** and designs so that they can target their resources effectively.

In all the years that Stile has been conducting these external tests, only one serious vulnerability has been encountered: in 2017 our testers found an XML eXternal Entity injection (XXE) in the third party WIRIS maths editor toolkit; the vulnerability was full quarantined within hours of discovery, and after working with the authors to fix the underlying vulnerability, the Stile engineering team fully removed all WIRIS software from Stile's systems. This vulnerability never exposed any user data.

Since then, Stile has consistently frustrated penetration testers by proving resilient to exploitation.

In addition to external penetration testing, Stile conducts internal 'red team' exercises where our own engineers attempt to break our systems using their detailed insider knowledge. These help to verify existing systems, put new designs to the test, and keep security at the forefront of our teams' minds.

Check out a recent external penetration testing report of Stile's production systems.

View report here

Note: findings classified as 'low' are informational and don't represent exploitable vulnerabilities. All findings have been discussed with the testers and fully mitigated.

Open Bug Bounty

Stile permits independent security researchers (ie. well-intentioned hackers) anywhere in the world to attempt to break into our systems, and offers them legal protection so long as they disclose any vulnerabilities back to us. We believe so strongly in the security of our systems that we offer a **bounty of up to fifty-thousand dollars** for finding a vulnerability.

Stile's vulnerability disclosure policy and bounty program are **available publically** and discoverable via the industry standard **security.txt** endpoint. Vulnerabilities can be sent to **security@stileeducation.com** where they will be triaged by our expert security engineers.

These policies allow us to harness the skills of the whole internet to find gaps in our security, ensuring that Stile provides the safest possible experience for all teachers and students.

System and Organization Controls (SOC2)

Stile is SOC2 compliant and audited.

SOC2 is an industry best practise standard for business operating with an extremely high level of availability, processing integrity, confidentiality, privacy, and security. The standard defines a high quality benchmark for risk identification and control measures, with appropriate management, oversight, review, and continuous improvement systems to keep the controls updated and effective.

SOC2 is very similar to ISO27001: Both standards require a best practice Information Security Management System (ISMS) and excellence in security, privacy and confidentiality. The notable differences are:

- SOC2 allows more flexibility for defining processes and controls appropriate to particular industries, rather than taking a one-size-fits all approach for all organisations
- SOC2 provides additional trust criteria for availability and processing integrity
- ISO27001 auditors must pass a certification exam and have audit experience, but SOC2 audits are conducted by specialised Certified Public Accountants (CPAs)

Stile's industry leading ISMS is externally audited and compliant with SOC2, and is designed to align with the ISO27001 standards, but hasn't yet been submitted for an external ISO27001 audit.

Check out a recent external SOC2 audit report covering all of Stile's systems and processes.

View report here

This report verifies both that Stile's systems and processesthey are sufficient to meet the SOC2 standards, and that they are implemented appropriately.



Data Processors

Stile sets a high quality bar for external suppliers of critical business components, and thus has relatively few of them. All suppliers must be vetted for data-handling, privacy, security compliance, suitability, total ownership cost, SOC2 compliance, and quality before being contracted. All suppliers are tracked centrally, and are regularly reviewed with a view to consolidation.

Stile shares personal information with these data processors only to provide and support the Stile service for schools. Stile never shares it for a sub-processor's own purposes. Each use described for each data processor is part of the primary purpose for which Stile collects the information, as permitted by **Australian Privacy Principle 6**. An overview of the data that can be shared with data processors is available in the **Data We Collect** section of this document.

Third party services which don't offer secure SSO integration are only used for non-sensitive tasks, and only if no alternative is available, and third party services which don't offer secure (non-SMS) multi factor authentication are strictly forbidden.

Special care is taken when vetting any services which will handle student and teacher data in any way. Use of external services for specialised tasks like server hosting, video transcoding, or email sending allows us to leverage industry expertise and reduce operational risk, but must be balanced against the increased surface area for attack. Stile aims to use only the most secure and reputable third party services, and is always looking for opportunities to consolidate and minimise.

Data Storage & Processing

The list of services storing student and teacher data is deliberately very short, thus minimising exposure to both external attack or internal mishandling. Both Amazon and Salesforce are the undisputed leaders in their field, and boast an unimpeachable track record. Data is stored with these services in Australia.

Amazon Web Services
Stile's services are all securely hosted by Amazon Web Services (AWS). All student data held by Stile is stored by AWS with strong isolation, access management, and at-rest encryption protections elaborated upon throughout this document.

Salesforce
Data about each of our schools, key teachers, and leadership contacts (but not students) is stored for Stile by Salesforce. Salesforce's systems are themselves hosted by AWS.

Transient Data Processing

These services do not store any student or teacher data, but may handle it temporarily when performing various processing tasks on Stile's behalf. Data is processed by these services in Australia or the United States.

Google
Stile analyses aggregated usage data using a privately hosted analytics suite from Google called Looker. Google does not store any data about our students or teachers, but does process it in order to format charts and reports on our behalf. All of these analytics services are themselves hosted in a dedicated AWS environment, managed by Google.

Microsoft Azure
Stile uses Microsoft's widely respected Azure cloud platform for a few services which aren't available at an equivalent level of quality from AWS, including experimental uses of generative artificial intelligence for assisting teachers.

OpenAI
OpenAI's generative artificial intelligence is used for assisting teachers within Stile, primarily to help manage ongoing updates to keep their lessons up-to-date, and to draft feedback for students if requested by teachers.

Mailchimp
Mailchimp sends email from Stile on our behalf, and thus handles any personal data included in those emails.

ChaosSearch
Search over audit and activity logs generated by the Stile Platform and its underlying infrastructure, enabling rapid investigation of operational issues, security incidents, and compliance-related events. ChaosSeach doesn't store Stile's log data, only handles it temporarily as it's accessed.

Ortto
Ortto sends email from Stile to teachers and schools on our behalf, and thus handles any personal data – like names – included in those emails.

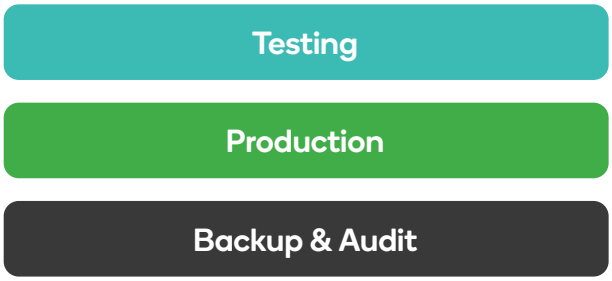
Intercom
Intercom provides support ticketing and issue management software to help us quickly respond to teachers that need help.

Zamzar
Zamzar helps us to convert Microsoft Office documents into PDFs for easy embedded viewing in Stile lessons.

Brightcove Zencoder
Zencoder optimises uploaded videos in Stile lessons so that they load quickly and without using too much network bandwidth.

Stile's Architecture

Stile is fully hosted by the industry leader in reliable and secure computing services: Amazon Web Services (AWS). Using separate AWS accounts – each with an isolated virtual network – Stile strictly segregates network access, permissions, and data storage between Development, Testing, Production, Backup and Audit and Sandbox environments. This allows us to rapidly deploy changes while minimising our exposure to attack, and protecting critical recovery data.



Network Security

Within each network, access between devices is denied by default, and specific ports are opened in each server's Firewall only on a strict as-needed minimum-privilege basis. Only a handful of extra hardened load-balancer servers are given public IP addresses exposed to the internet - all other servers are connected to each other only as-needed via a private subnet.

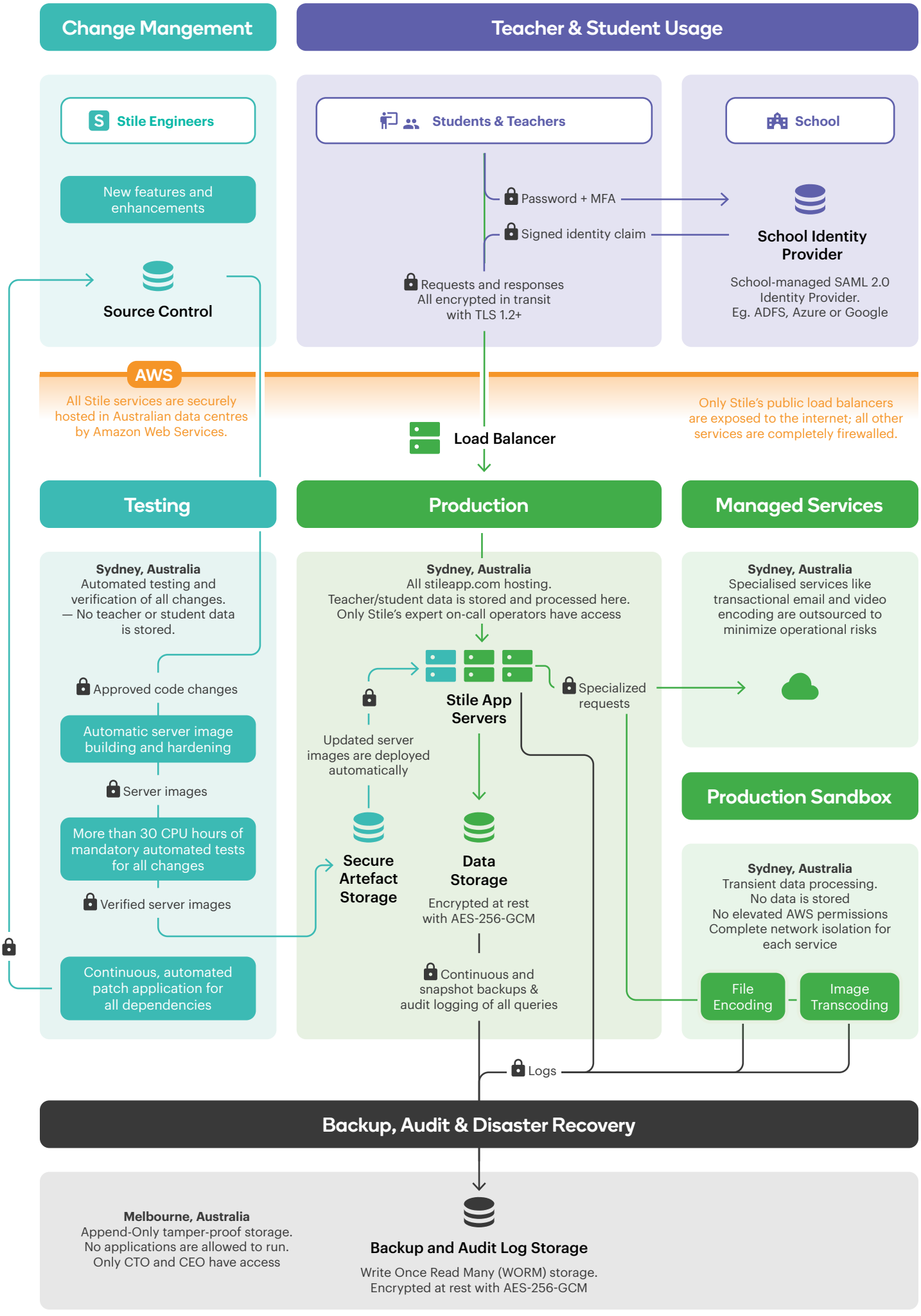
Student and teacher data is never moved or copied into development or testing environments.

All networking configurations are managed as code (via Terraform), committed to source control (Github) and subject to automated testing and manual review, thus minimising the risk of configuration error and ensuring conformity to policy.

Metrics about all network requests and data transfers are continuously recorded and monitored for anomalies which may indicate availability or security problems. Stile's Network Intrusion Detection System (NIDS) monitors all network traffic (internal and external) for anomalies or suspicious patterns and alerts one of Stile's 24/7 on-call engineers to investigate and respond to any potential malicious activity.

Stile's offices in Melbourne and Portland provide private networks which allow internet access for staff, but don't allow any privileged access to Stile's services or data. That means that a compromise to the physical security of our offices wouldn't lead to a compromise of any Stile services.

Access to Stile internal services always requires both privileged network access via Stile's staff Virtual Private Network (VPN), and explicit zero-trust Role-Based Access Control (RBAC) to the internal service. Access to Stile's VPN alone doesn't grant any privileged access. All access to internal services is controlled and provisioned centrally through Stile's internal Google Workspace identity provider, which enforces strong multi factor authentication (through tamper-proof hardware U2F/FIDO/Webauthn/Yubikey tokens) as well as leveraging Google's industry leading threat identification and protection systems to respond to suspicious activity.


Change Mangement
Teacher & Student Usage
Stile Engineers
New features and enhancements
Source Control
Students & Teachers
Password + MFA
Signed identity claim
Requests and responses
All encrypted in transit
with TLS 1.2+
School
School Identity Provider
School-managed SAML 2.0 Identity Provider.
Eg. ADFS, Azure or Google
AWS
All Stile services are securely hosted in Australian data centres by Amazon Web Services.
Load Balancer
Only Stile's public load balancers are exposed to the internet; all other services are completely firewalled.
Testing
Production
Managed Services
Sydney, Australia
Automated testing and verification of all changes.
— No teacher or student data is stored.
Approved code changes
Automatic server image building and hardening
Server images
More than 30 CPU hours of mandatory automated tests for all changes
Verified server images
Continuous, automated patch application for all dependencies
Sydney, Australia
All stileapp.com hosting.
Teacher/student data is stored and processed here.
Only Stile's expert on-call operators have access
Stile App Servers
Updated server images are deployed automatically
Specialized requests
Secure Artefact Storage
Data Storage
Encrypted at rest with AES-256-GCM
Continuous and snapshot backups & audit logging of all queries
Sydney, Australia
Specialised services like transactional email and video encoding are outsourced to minimize operational risks
Production Sandbox
Sydney, Australia
Transient data processing.
No data is stored
No elevated AWS permissions
Complete network isolation for each service
File Encoding
Image Transcoding
Logs
Backup, Audit & Disaster Recovery
Melbourne, Australia
Append-Only tamper-proof storage.
No applications are allowed to run.
Only CTO and CEO have access
Backup and Audit Log Storage
Write Once Read Many (WORM) storage.
Encrypted at rest with AES-256-GCM

Incident Response

What happens when there's a problem?

Stile's team of teaching experts – based in Melbourne – are always available during school hours by phone, email, and in-platform messaging. Email queries are typically responded to within 10 minutes, and resolved in under an hour. Phone queries are typically resolved immediately. We successfully resolve more than 7,000 teacher queries each year.

Stile is further supported by our staff of Melbourne-based expert on-call engineers who provide 24/7 support for any issues that can't be resolved immediately by our support team. A sophisticated suite of more than 300 hand-tuned automatic alerts – drawing on more than 20 million time series metrics collected every 15 seconds and describing every aspect of Stile's operations – ensure that an on-call engineer responds to and fixes the vast majority of incidents before any teachers or students even notice. This same 24/7 on-call process with automated alerting also ensures that any security incidents are proactively detected and mitigated before they can escalate.

Emergency responses follow Stile's well documented Incident Response Plan, including separating Incident Controller, Communications Officer, and Subject Matter Expert roles; automatic escalation of serious or unresolved issues up through the chain all the way to the CEO; and blameless post-mortem and periodic incident review meetings to uncover trends and systematic improvements. All incidents are automatically recorded, and labelled by the incident controller for long term trend analysis.

As part of Stile's at-least annual Disaster Recovery Testing Exercises, several extreme scenarios are simulated, providing excellent training for our team, and ensuring that all response plans, incident management procedures, tools and processes are effective.

Action items for improvement resulting from incidents, near-incidents, post-mortem reviews, trend analysis, and disaster simulations are always actioned within 21 days. Stile implements – on average – 218 such systemic improvements per year, resulting from an average of 14 comprehensive blameless post-mortem inquiries, and 26 incident review meetings.

Staff Access

Strong security and privacy controls within Stile's organisation are just as important as protecting your information from external attack. Stile staff do not have access to personal data unless strictly required for their role. Some Stile staff need access to personal data in order to help set up new schools, resolve teacher queries, and fix technical problems with our systems. Such access is only permitted to thoroughly vetted employees – never to contractors or third parties – and is only granted on an as-needed basis for each staff member's role. Critically, *support access is only ever allowed with explicit permission from an authorised teacher*. All such staff access – including emergency direct database access by Stile's on-call engineers – is logged and audited to ensure appropriateness and to facilitate incident investigation.

All staff access to internal systems (including casual staff and contractors) is managed centrally with Role Based Access Control (RBAC), through SSO provided by Google Workspace or Okta with mandatory Hardware Multi Factor Authentication (MFA/2FA). A strong data classification system ensures that teacher and student data is only stored in appropriate systems with strictly restricted access. Staff are given only the minimal permissions to each system that they need in order to do their job. Staff access is audited at least quarterly to ensure that this minimal-access principal is being properly followed.

All staff access is performed through an auditable personal account. **Shared accounts are strictly forbidden**, and hardware security tokens (Yubikeys in U2F/FIDO/Webauthn mode) make account sharing impractical in any case.

Root access to Stile's production and backup environments is only available with one of two special hardware tokens, securely and separately stored offsite by the CTO and Deputy-CEO. These root accounts are only ever used for emergency recovery, never as part of day-to-day operations.

All staff receive specialised security training both as part of their induction, and on an ongoing at-least-annual basis. This training focuses on the most critical emerging threats, and is backed by ongoing review and support from Stile's security and management teams to ensure that best practices (eg. use of long, unique, randomly generated passwords for all accounts, kept in a password manager) are being diligently followed.

Stile staff are thoroughly vetted upon hiring: background checks, and **Australian Working With Children** checks complement our **thorough hiring process**, which includes reference checks and three rounds of panel interviews.

Upon termination, all staff access is terminated within minutes. Within 24 hours, access revocation to **every service** is manually checked by our IT team, then verified by a senior member of our Security team, and a member of our People and Culture team.

Stile Staff Security

Staff Management

Rigorous Interview Process → Reference Checks

Background, Working with Children, and Police Checks

Security & Privacy Onboarding

Role Based Access Control
Managed centrally via Google Workspace

- No access
- Access
  - Operations
  - Support



Oversight & Review

Executive approval

Risk review

Annual training addresses emerging risks

Same day offboarding

Offboarding double-checked by security and P&C teams

Quarterly review of all staff roles and access levels

Data Access

Operational incident → Explicit, authenticated personal data access permission

Support request → Explicit, authenticated personal data access permission

Hardened employee devices

Hardware 2nd factor authentication

Virtual Private Network

Operators and Support staff fulfill support requests by accessing data through Stile's main API's over a special VPN-only endpoint

Stile API Servers

Stile's servers log all requests and responses

Operators can directly access the database when necessary as a 'break glass' action which triggers alerts visible to all staff

Teacher and student data

The database directly logs all queries (from both the API servers, and operators)



Device Management
Ensures up-to-date operating systems, consistent hardened configuration, strong encryption, strong passwords. Allows for remote locking and wiping of lost devices

VPN access is logged

Logging, Metrics & Alerting

Staff access logs are kept for 7 years

'Break Glass' access is posted internally for all staff to review

Monthly access log audit

Frequently Asked Questions

Below are answers to some of the most common questions that schools leaders, ICT executives, and security experts ask about Stile. The responses dig into some technical details, but there's always more to the story. We love talking about security, so feel free to reach out to your account manager or **support@stileeducation.com** if you have any questions which aren't answered here.

How does Stile manage changes to its systems?

Stile's industry leading change-management process makes extensive use of automated testing, automated monitoring and manual review to ensure the highest quality standards are consistently met. Key steps in the change-release process are as follows:

- Significant changes are initially planned in a Technical Requirements Description (TRD) document which is reviewed, enhanced and approved by senior engineering staff before work begins. Security and privacy are core design objectives that must be embodied in every planned change.
- All of Stile's services and technical documentation (including TRDs) are managed through a central Version Control System (VCS), which allows all changes to be identified with a snapshot of the system code. Stile's VCS is a single large git mono-repository hosted on Github.
- All changes – represented by a VCS snapshot – are manually tested in a development environment before being submitted for review.
- Before manual review and deployment, every submitted change must pass an **extensive suite of automated tests running for more than 30 hours** (highly parallelised to reduce the actual wait time down to minutes). These tests cover every part of the system without exception, and include:
  - Automatic enforcement of coding and security standards
  - Unit testing of every system component in isolation
  - Integration testing of all server-side systems
  - Integration testing with real 3rd party service provider APIs
  - Integration testing of the server and client systems together, including user-simulation via browser automation, and visual-difference testing
  - Fault-injection testing in a simulated deployment environment
  - Testing for injection vulnerabilities with known malicious payloads
  - Thoroughly exercising all of the internal authorisation and access control logic which power's Stile's private-by-default experience

- All proposed changes are reviewed by engineers before being deployed. This process isn't just a formality: it regularly prompts discussion that generates significant enhancements or design changes.
- Merging of changes is fully linearised in batches by Stile's automated merge queueing system. This ensures that all interactions between changes are hands-off tested before release.
- Fully reviewed, tested, and merged changes are all deployed with a fully automated blue-green process multiple times per day, allowing rapid iteration and minimising the deployment risk from large change-sets:
  1. The changed system is provisioned as a completely separate production environment
  2. All core functionality is tested in the new environment with built-in health monitoring systems and browser automation testing
  3. Then – only once the new system is confirmed to be working as expected – live traffic is transferred to the new system and key metrics are monitored for anomalous behaviour (which may indicate unexpected problems with the changes)
  4. If there is any unexpected behaviour from the new system, then traffic is redirected to the old system immediately to ensure uninterrupted service delivery while the anomaly is manually investigated by one of Stile's 24/7 on-call engineers.
  5. The old production environment will be de-provisioned only once the new system has been running reliably under significant load for at least 30 minutes
- All systems report extensive log, trace and metric data, describing the health of internal system processes, any unexpected events, and tracking the completion of expected workflows (request rates, response times, sign-in rates, usage of various features etc.). This data is used to ensure correctness in the development and testing phases, and to allow rapid, informed responses to incidents in production.
- Deployed systems are actively monitored for abnormalities and security-scanned/fuzz-tested for vulnerabilities, allowing us to rapidly detect any problems which have made it through to this point.
- Once deployed, changes are reviewed by another engineer to ensure that the requirements have been correctly addressed.
- A sample of deployed changes are re-reviewed internally by senior engineers and managers to audit for quality standards, and by groups of engineers as a learning exercise.
- Deployed features are tested internally and with teachers in our previewer program before being generally released (note: releasing new features is a separate step from deploying them, and can be instantly controlled by Stile's product team). This ensures that newly released features always work as expected in real classroom environments.

Inclusive, blameless post-mortem analyses are regularly used by all teams at Stile to analyse incidents and near-incidents retrospectively. The recommendations of these reviews are reliably tracked and always actioned within 28 days.

Stile's agile content and platform development processes deliver incremental value to teachers at regular intervals (at least every two weeks). This ensures that feedback can be regularly gathered over the lifetime of a project to steer it towards delivering maximum value for teachers, or to change direction radically if the desired results aren't being achieved. After a two week period, each team reviews their own work and develops process improvements to be implemented in the next cycle.

Does Stile encrypt all data at rest and in transit?

Yes. **Stile encrypts all data in transit** using only exhaustively tested, audited implementations of modern, secure ciphers (`AES–GCM–SHA2` and `CHACHA20–POLY1305–SHA2`) and protocols (TLS 1.2+). **All data at rest is encrypted** with AES-GCM-SHA256.

These ciphers and protocols are frequently updated in keeping with industry best practice and emerging threats.

Stile does not accept any unencrypted HTTP traffic and uses HTTP Strict Transport Security (HSTS) preloading to ensure that all clients connect security over HTTPS. The **best modern SSL best practices** are used to ensure that all data is kept secure in transit.

Stile employs the misuse-resistant cryptography library libsodium (via the **RbNaCl library**) to securely encrypt (and authenticate) backup files. Stile does not roll its own cryptography or cryptographic protocols.

How does Stile protect passwords?

Stile strongly encourages all schools and districts to **configure Single Sign On (SSO)** using SAML 2.0 (or OAuth2 for login with Microsoft or Clever). All SSO integrations are performed using well tested, popular open source libraries, minimising the risk of implementation errors. SSO users never send their passwords to Stile.

Passwords for non-SSO users are securely stored using the specially designed slow-hash function bcrypt2. This makes it infeasible to reverse-engineer our stored password data to retrieve any part of the original password.

Stile continuously monitors all sign-in attempts and automatically responds to suspected abuse, including both repeated attempts to guess a single account's password, and credential-stuffing attacks where common passwords are tested against many different user accounts. This automated response includes escalating to one of Stile's 24/7 on-call engineers to investigate and respond to potentially coordinated malicious activity.

Because Stile doesn't keep plaintext passwords, we never send passwords to users. Passwords are created by users during sign-up (never generated by Stile), and password resets are performed by sending a reset link via email.

How does Stile secure session tokens?

When a teacher or student logs into Stile, they receive a session token (generated using a Secure Pseudo-Random Number Generator) and include this token with future requests to prove their identity. These session tokens are **not** stored (or accepted) as cookies, and so Stile isn't vulnerable to Cross-Site Request Forgery (CSRF/XSRF) attacks.

These sessions are only retained in secure on device storage and never moved between devices.

Session tokens expire after a short period of inactivity, ensuring that students and teachers must periodically re-authenticate (potentially fetching any new attributes and updated privileges from their SSO identity provider). Stile allows users to see and revoke all active sessions for their account, and permanently expires sessions on logout. Only a small number of active sessions can be maintained at a time - generating newer sessions will invalidate older ones to reduce the risk of lost tokens from old devices etc.

How does Stile protect against Cross Site Scripting (XSS) Cross Site Script inclusion (XSSI) attacks?

Stile's frontend is built using React, a modern secure-by-default framework that automatically escapes all rendered data. User generated rich text is stored in JSON format (in a schema defined by the ProseMirror text editor), which prevents any injection of arbitrary code or HTML tags by design.

Some legacy user-generated text is stored as HTML and sanitised by Stile's servers (using a limited allowlist of supported tags and attributes) before being served.

All responses from Stile's APIs include the following headers:

```
Content-Security-Policy: "sandbox"
Content-Type: "application/json"
X-Content-Type-Options: "nosniff"
```

which work together to ensure that nothing from Stile's APIs will be interpreted as executable code, and that Stile's APIs can't be used to reflect harmful payloads. All media assets served by Stile – including all user-uploaded files – come with similar sandboxing headers with the relevant server-determined image, video etc. content-types.

Only requests for Stile's static javascript and HTML assets allow browsers to execute/render data in the response.

All pages are served with a `Content-Security-Policy` header that limits script and media sources to only trusted domains. Stile enforces strict same-origin browser policies wherever possible.

Stile does not make use of JSONP or any server injected format which could expose it to script-inclusion attacks.

How does Stile protect against Clickjacking attacks?

Stile uses the `X-Frame-Options` and `Content-Security-Policy frame-ancestors` headers to forbid loading any part of Stile in an iframe so that users can't be tricked into interacting with Stile by accident.

How does Stile protect against SQL Injection attacks?

All SQL queries are generated using a secure query builder library which escapes all input by default. String substitution/concatenation is never used to construct queries. Proper escaping is enforced by code review assisted by automated code analysis, and verified by fuzz testing with known injection attacks, both during development, and continuously against production APIs.

How does Stile protect against Server Side Request Forgery (SSRF) attacks?

Stile uses a layered, defence-in-depth approach to protect against SSRF attacks:

- Network requests made by Stile's servers which accept user-specified URIs (eg. directly uploading a file to Stile via the Microsoft Onedrive OAuth integration) use strict hard-coded allowlists to filter for only safe hostnames.
- XML parsing is only performed using an audited, secure-by-default library which ignores external entities, thus protecting against XML eXternal Entity injection (XXE) attacks.
- Outbound internet requests from Stile's servers are performed via a secure, but unprivileged HTTP proxy server running outside of Stile's internal network. This means that these requests do not get any privileged network access by default, and don't appear to originate from Stile's application servers directly. These unprivileged proxy servers do not have stable IP addresses, preventing anyone from mistakenly trusting network traffic from them.
- All network access is strictly limited to only allow minimum required access between servers, thus limiting the potential blast radius of any SSRF vulnerability.
- All sensitive HTTP interfaces – both in Stile's own APIs, and in our internal infrastructure – require PUT/POST/DELETE HTTP verbs, which are harder to generate even if a successful SSRF exploit is uncovered. This includes mandatory use of Amazon's Instance MetaData Service V2 (IMDSv2) endpoints on all servers to protect server metadata.
- Finally, Stile's NIDS monitors all traffic for anomalies or suspicious patterns and alerts one of Stile's 24/7 on-call engineers to investigate and respond.

How does Stile secure user uploaded files?

Stile allows students and teachers to upload multimedia files to facilitate rich multi-modal learning and project work.

Students can only upload files when requested by their teacher, and once uploaded, those can only be accessed by that teacher. Files uploaded by a teacher can only be seen by their students when the teacher releases the relevant lesson.

To minimise the risks from malicious file content, **Stile virus scans all uploaded files** and automatically quarantines suspicious files for later analysis.

All images, video and document files are re-encoded by Stile for security and efficiency, thus limiting the possibilities for malicious payloads to be disguised in a media file. Documents are converted (to PDF), and videos are re-encoded by hosted services, which eliminates the possibility of decoder vulnerabilities affecting Stile's infrastructure.

All image transcoding (and other inherently risky data processing) is conducted in a fully isolated AWS account (separate from other production services) by single-purpose, hardened, stateless servers with no privileged data or network access, and only temporary working access to each uploaded file. These servers, their operating systems and the image transcoding software that they run (Imagemagick) are kept up to date and regularly replaced. This maximally reduces the scope for damage from any potential vulnerabilities in our file-handling software.

Stile always serves uploaded files with the `Content-Security-Policy: sandbox` header – to prevent browsers from executing any scripts embedded in the file – and serves them from a separate domain (**uploads.stileapp.com**) from all pages and APIs to ensure that same-origin rules would separate sensitive data even if a script was executed. Stile's web client application never deeply inspects or executes any content from user uploaded files; they are simply displayed by the browser.

Is all software kept up-to-date?

Patches to all Stile systems – including software libraries, operating systems, system packages and portable binary tools – are applied automatically, verified by our continuous integration system and deployed to production automatically. All patches are automatically triaged according to the criticality and risk levels of the systems they affect, and taking into account any known CVEs; high priority patches are closely monitored to ensure that they are applied quickly and without error.

Stile internally commits to keeping all infrastructure fully updated within 14 days, with more critical user-facing systems being updated many times per day. This minimises exposure to risks from unpatched vulnerabilities in operating systems, third party software, and configuration drift, even when vulnerabilities haven't yet been announced.

The vast majority of patches are deployed to Stile's production systems within 24 hours of release.

This rapid, automated updating ensures that Stile's systems are already hardened against the vast majority of vulnerabilities in third party software that we depend on before they are publicly known, minimising the window for exploitation.

How are Stile's servers hardened against vulnerabilities?

Automation allows perfect reproducibility of Stile's thorough system-wide hardening process.

All software dependencies are fetched through Stile's internal mirror, minimising our exposure to compromise or outage from third party software distribution services. Every software dependency (operating systems, system packages, application libraries etc.) is **pinned to an exact version** in Stile's source control system. Our sophisticated continuous integration pipeline rebuilds all software – operating system images, docker images, and application software – from source in response to every change, automatically configures all servers according to Stile's robust hardening process, and scans for vulnerabilities before running more than 30 hours of automated tests (massively parallelised to reduce the actual wait time down to minutes) to verify all aspects of the system are behaving as expected.

All cloud system configurations are controlled by Terraform code, tracked in Stile's global source control mono-repository, and subjected to manual review and automated testing, thus ensuring perfect reproducibility of any running infrastructure, including all hardened AWS network and service rules. Stile enforces a uniform, immutable, blue-green deploy process for all infrastructure, allowing each incoming system to be fully tested and verified before promoting it and cleaning up the old copy.

How are staff devices secured?

We approach internal security in the same way that we approach security for Stile teachers and students: making sure that the experience is both **delightful** and **secure by default**. Security is core to what we do, not an external imposition that staff work around in order to get their jobs done.

All staff devices use biometrics (Apple TouchId) to allow quick convenient access to locked devices during the day: this removes the usual inconvenience of long passwords and short screen-lock timeouts, making security something that our staff can easily embrace, rather than a constant irritant.

Stile staff devices are all encrypted with strong passwords and centrally managed and tracked by Stile's security team. Centrally policies enforce password strength (at least 14 characters + a high complexity threshold) and short automatic locking times (at most 5 minutes). Lost devices can be remotely locked or wiped by our security team.

Our hardware asset register of devices is updated automatically by our device management tools, including tracking operating system and software updates. The asset register is manually double-checked at least quarterly.

How is our data backed-up?

Stile targets 99.99% data recoverability once it has been positively acknowledged by our APIs, and 100% recoverability within 24 hours afterwards. This means that as soon as you enter data into Stile and it shows as 'saved', you can expect the data to be stored securely and reliably.

Stile has a perfect track record for meeting this target since its founding in 2012.

All systems are engineered from the ground up to ensure that acknowledged data is persisted to disk, replicated multiple times, and backed-up to guard against loss or corruption. This includes capturing database replication logs of all changes, database audit logs of all queries, and application level snapshots of all changed objects, all of which are replicated to an isolated production environment (a separate AWS account) where they can't be deleted or tampered with, including by Stile staff. In addition to our primary backups across all Sydney/Oregon AWS data centres, we store secondary copies of critical data in the Melbourne/California AWS data centres, allowing recovery even in the event of an extended, region-wide outage.

Backups are automatically verified, and restoration is tested at least quarterly.

Does Stile keep logs of activity in its systems?

Stile records detailed audit logs of all requests made to Stile's servers, all actions taken within the application, all changes to key objects, and all queries made against Stile's databases. Even more detailed and replicated logging is collected about sensitive actions (e.g. adding teachers to a school).

All actions by Stile staff (both in the platform, and in the provision and maintenance of Stile's infrastructure) are also logged with the staff member's id attached. Logs of Stile staff activities are periodically audited to ensure compliance with internal policies.

All logs have detailed records of session ids, IP addresses, and other client information, as well as correlation ids to allow causally related logs to be aggregated together. This ensures that malicious activity can be tracked and isolated with high precision. Logs are all kept for 7 years and fully-indexed for quick search when investigating an incident.

It is impossible for all copies of a log message to be modified or deleted by an attacker who has gained access to Stile's production systems.

All application, operational, infrastructure, system, audit, and database logs are immediately copied into a secondary AWS account in a secondary geographic region (in Melbourne for Australian data, and California for US data) which allows append-only access, and which no Stile staff have control over during the normal course of business. AWS policies are configured to prevent the deletion of log data for at least 7 years, even with access to the account. No code or other systems are allowed to run in this account or with privileged access to it (ensuring that the account isn't exposed to remote code execution attacks or any other software vulnerabilities), and no staff have credentials allowing modification of data or settings in the account (ensuring that tampering is impossible, even if privileged staff credentials are lost). Modifications to this account or data within it are only possible using one of two physical hardware keys, stored in separate offsite secure safes by the CTO and Deputy CEO.

This ensures that even in the event of a significant breach of Stile's systems, the actions of an attacker could be tracked and isolated.

All backups and application level object-snapshot events are stored using the same tamper-proof system. This ensures that not only can the consequences of any action be traced using this secure log data, but any unwanted effects can always be reverted to a point in time immediately before the action took place.

Call us on 1300 918 292

Email us at community@stileeducation.com

Swing by the office to say hi!
Level 5, 128 Exhibition Street, Melbourne, Victoria

Stile HQ is located on the traditional lands of the Boon Wurrung and Woiwurrung (Wurundjeri) peoples of the Kulin Nation. We acknowledge that sovereignty was never ceded and pay our respects to Elders past, present and future.