Security Measures

Last Updated: 1st September 2024 - Revision 9

This document describes the organisation and technical measures implemented by Schoolbox Pty Ltd (Schoolbox) in order to protect personal data and ensure confidentiality, integrity and availability for the Schoolbox Software.

This document covers only the measures implemented by Schoolbox, where data is handled by sub-contractors or subprocessors we have separate agreements in place. Please refer to the Subprocessor List for detailed information about these providers and their terms of service.

Where the Schoolbox Software is Self-Hosted, it is important to remember that you, the Customer, are also responsible for data protection. For more information on the steps required to protect your data when self-hosting please review our self-hosted security guide.

From time to time Schoolbox may change these measures. This may mean that we replace existing measures with new measures or implement entirely new measures. The intent of these changes will never degrade overall security, but improve or evolve protocols to deal with new or emerging threats, changes to laws or regulations or adopting of new security standards.

Within this document, the following definitions apply:

- "Customer" means any Licensee of the Schoolbox Software.
- "Schoolbox Software" means the Schoolbox software products licensed by Schoolbox to the Customer pursuant to a Service Agreement and includes:
    - Schoolbox Self-Hosted – Schoolbox software installed on your infrastructure;
    - Schoolbox Hosted – Schoolbox software hosted on our cloud platform; and
    - Self-Hosted Add-Ons: Hosted Backup (ADHB) & Hosted Storage (ADHS).
- "Personal Data" means any information provided or submitted by the Customer or Customer's authorised users in connection with use of the Schoolbox Software, in each case relating to any identified or identifiable natural person, that Schoolbox processes on behalf of Customer.
- "Personnel" all Schoolbox employees (permanent, contract, casual, full-time and part-time), Schoolbox's contractors and any other people or organisations working for Schoolbox or on our behalf.

Organisational Information Security

As an organisation we have implemented a security framework that is ratified and supported by leadership and ensures all Personnel are competent and aware of their responsibilities towards information security.

Measures include:

- Schoolbox has information security policies, approved by senior management and disseminated to all Personnel.
- Schoolbox security policies are reviewed at least annually and updated as required.
- All Personnel with access to confidential data will be bound by confidentiality clauses appropriate for their role and the data to which they have access.
- All Personnel must agree to and sign an “Acknowledgement of Policies” that are designed to ensure Personnel understands and follows Schoolbox’s information security rules.
- Failure of Personnel to follow information security policies may be treated as a disciplinary matter and lead to sanctions.
- All Personnel are given initial training in information security and thereafter at least annually. Personnel in specific roles may take part in role-based security training relevant to their position.
- Information security is part of the culture, we are aware of our responsibility and duty of care and ensure that all software is designed and architected in accordance with our responsibilities.
- We seek external assistance and training to ensure the continual improvement of our security.
- We welcome external review, analysis and feedback. We have adopted a responsible disclosure policy and accept reports via security@schoolbox.education.

Physical Security

To protect your data from physical access by unauthorised personnel. These measures cover data stored by Schoolbox and do not cover where the customer is self-hosting their own data.

Measures include:

- Schoolbox utilises AWS data centres to store customer data, further information regarding the physical protections provided by AWS.
- Which data centre your data the software is hosted within, can be found in our Where is my Schoolbox instance located?
- Customers may choose which country they prefer their data to physically reside within from our existing availability zones.
- Schoolbox ensures all data is encrypted at rest within AWS to ensure that physical access would not allow access to the data.
- The Schoolbox offices in Melbourne, Australia are protected by key card entry and surveillance systems. No Personal Data is physically stored in the offices.
- Any Schoolbox data devices (hard drives, memory sticks) at the end of their life are wiped or physically destroyed before being disposed of.

System Access

Schoolbox data processing systems are accessed and used only by approved Personnel.

Measures include:

- Access to Schoolbox internal systems is granted only to currently employed Personnel and access is limited as required for those persons to fulfil their function.
- Schoolbox requires internal systems to connect via SSO to our identity system. Our identity system centralises control of accounts and ensures consistent policy across all internal systems.
- Schoolbox has established a password policy that prohibits the sharing of passwords and ensures the use of strong passwords.
- Schoolbox requires that all Personnel utilise MFA for authentication to our systems. The MFA must be either a mobile app or YubiKey.
- Each computer has a password-protected screensaver.
- If required by their role, Personnel may have access to a customer Schoolbox instance in order to provide support. This access is only utilised on an as-needed basis in order to deliver upon the service levels covered in our Schoolbox Support Policy.
- In order to access internal systems our Personnel must first be connected to our internal network, either by being physically present in a Schoolbox office, or via encrypted VPN, which can only be connected to from pre-approved devices.
- Schoolbox has a thorough procedure to deactivate users and their access when a user leaves the company or to alter their access rights if their job function has changed.

System Updates

To protect our systems from exploitation due to publicly known vulnerabilities we will ensure all our systems are running the latest security updates.

Measures Include:

- Ensuring that all operating systems within the organisation are currently supported with security releases
- We ensure that appropriate Personnel receive alerts and notifications from system software vendors and other sources of security advisories and install system software patches regularly and efficiently.
- Updates are sourced from industry standard repositories that are validated and authorised.
- Staff monitor the roll out of updates across the fleet to ensure completeness of application.
- We utilised a centralised configuration control system to ensure that all systems meet the minimum patch level.
- Review product dependencies every 6 months to ensure we are running the highest compatible versions and make appropriate changes to ensure we remain on supported versions.
- We ensure all Personnel are running up to date software on their devices
- We ensure all Personnel are running up to date anti-malware software on their devices.

Data Access

In order to provide our customers with high quality support services, we may require access to customer data in order to help diagnose issues, provide training services and migrate data. We recognise that with this access we have a great deal of responsibility to protect the data that customers have entrusted to us.

Measures include:

- Schoolbox has a policy that data will only be accessed on as needed basis, it will never be accessed for any other purposes other than to provide our services as requested.
- Schoolbox has a policy that customer data will never be exfiltrated or moved from its primary location unless explicitly requested or authorised by the customer.
- Our Personnel will never share Personal Data with unauthorised persons, only nominated people within your organisation can access Schoolbox support, and communicate with our Personnel.
- All Personnel with access to data have had appropriate background checks of at least Working With Children Check (Victoria) or equivalent standard.
- Schoolbox may collect usage data regarding the system, but this data will always be anonymised and will have never include any identifiable information
- All access to the servers running Schoolbox is secured via one-time use encryption keys. These keys allow SSH access to our managed infrastructure and are provided on an as needs basis only.

Data Transmission

When data is being transmitted across networks, specifically public networks like the internet, it is at risk of being intercepted, manipulated or stolen during transfer.

Measures include:

- When transferring data over the internet we will utilise HTTPS TLS 1.2+ for web traffic and SSHv2 for all other traffic
- In order to establish trust all Schoolbox instances have signed LetsEncrypt certificates, these certificates are automatically provisioned and renewed every 2 months (Schoolbox does not support the use of less secure Wildcard or manually generated certificates)
- We recommend that customers only allow remote SSH access to their servers via our predefined network IP addresses to ensure only our Personnel are able to connect.
- If possible we will avoid sharing secrets and certificates. Where it is not possible secrets will be shared via one-time use only links.
- Personal Data may be required to be transmitted in bulk (for example, during an initial implementation, audit or data return). This will be facilitated through the use of encrypted files shared via controlled access sharing. Share links will be set to expire after a short period, and decryption passwords shared via a separate communication medium to the sharing link (e.g. emailed link, verbally provided password).

- Any data shared with us or shared by us will be destroyed within 7 days to ensure that Personal Data is not held in unprotected locations.

Development Process

Schoolbox implements administrative and technical controls to ensure that all code developed is designed, architected and delivered in the most secure ways possible.

Measures Include:

- Schoolbox utilises a defence in depth approach. This means security is built into the product at multiple levels, so that if a single level fails there are extra safe guards in place.
- When gathering requirements and designing functionality we employ senior positions including System Architects and Product Owners to ensure solutions are secure by design and that applicable security standards are incorporated into our architecture and solutions.
- Schoolbox trains all development engineers in secure coding practices. This includes awareness of standard exploits, best practices and how to test for security issues.
- Schoolbox has a central repository of code that is only accessible to authorised Personnel. All code contributions to this repository must be reviewed by senior development engineers and pass multiple automated checks before it is authorised to be part of a release.
- Schoolbox has automatic scanning of code dependencies for vulnerabilities and supply chain exploits and regularly updates packages. This is built into Schoolbox's code repository configuration.
- Schoolbox annually conducts penetration/vulnerability tests for common OWASP exploits, utilising industry standard tools that provide both automated and manual testing configurations.
- The release process is fully automated and must pass a series of automated testing suites before passing. It requires at least two senior Personnel to complete. Releases must first be delivered to staging environments successfully before they can be deployed to production.
- The Schoolbox product will be updated regularly on an as needed basis. Typically minor releases will be fortnightly and major releases will be 6 monthly.
- Minor releases will be announced 24 hours prior to the production release. The will be available in staging environments immediately following the announcement.
- Major releases will be announced at least 2 weeks prior to final release and will be deployed to staging environments during this period. When they pass final testing they will be announced as gold and deployed to production environments.
- Customers with Self-Hosted environments are required to book upgrades, failure to deploy these updates in a timely manner may result in degradation of security.
- Schoolbox uses a combination of automated testing (via unit tests and smoke tests, built in a continuous integration pipeline) and manual testing conducted by experienced Test Engineers on all new and modified code

Availability and Data Sovereignty

Schoolbox takes a number of steps to ensure your data remains protected from accidental destruction or loss. Schoolbox ensures that you have access to your data and that it can be exfiltrated from our systems if required.

Measures include:

- The Personal Data you provide to Schoolbox remains your property, we do not claim ownership or control over your data. You are responsible for the data that you store in our systems, you must ensure that it does not infringe on the rights or privacy of any other parties, and it is held in accordance with relevant privacy legislation.
- Schoolbox has business continuity plans in place to manage the risk of key Personnel and infrastructure incidents.
- Schoolbox will make best efforts to ensure you have access to your data via APIs and exports. Where these are insufficient you may request your data is exported and provided to you in standard formats.
- Prior to termination, you may request that we provide you with a backup of your data and we will take all reasonable steps to provide it to you.
- At the termination of your Schoolbox contract, your data will be made accessible to you for a period of at least 30 days although upon request we can retain this data for a period of up to three months, after which time it will be erased from production and staging systems.
- Schoolbox has made commitments to comply with all laws applicable to the provision of the services by us including applicable privacy laws

Measures for Schoolbox Hosted Customers:

- We will backup your data to one other location. The backup will be taken daily, and we will keep backups at reducing frequency up to 2 years.
- We will store your data in highly fault tolerant systems with at least 2 availability zones. In the event that one availability zone becomes unavailable your data will be made available from the other location.
- We will make best efforts to provide data hosting in availability zones that represent your legal jurisdiction. Where that cannot be achieved, you the Customer may choose the location from our availability zones that best aligns with your legal requirements.

Data Separation

Personal Data from one Customer is always logically separated from that of other Customers. These measures only apply to Schoolbox Hosted Customers.

Measures include:

- Each Customer has their own database with no ability to access data in other customers' databases.
- File storage is logically separated for each customer.
- Each Customer has their own unique secrets and credentials to ensure that their access cannot be used to access the database or files of other customers.
- The Schoolbox staging infrastructure is separated from the production infrastructure

- The development engineers utilise isolated environments for testing. These environments do not utilise any Personal or Customer Data.
- The Customer may request data is synchronised from production to staging on demand, our Personnel only completes this action with express permission from authorised contacts at the Customer, preferably in writing.
- The infrastructure logs, metrics and usage data is centralised for the purposes of monitoring and observation. We take all reasonable precautions to anonymise this data where possible, however it may from time to time contain Personal Data for the purposes of auditing and identification of system faults or errors.
- If we provide access to data for the purposes of auditing to Customers we will ensure data provided is related to the requesting customer only.

Incident Management

In the event of any security breach of Personal Data, the effect of the breach is minimised and the Customer is promptly informed.

Measures Include:

- Schoolbox maintains a data breach response plan and a process for how to assess events for various types of incident classification and escalation.
- The usual notification periods for updates will be waived in the event of a serious security incident and updates may be deployed immediately to mitigate any further security incidents.
- Schoolbox maintains detailed audit logs and ensures time is synchronised across systems to facilitate forensic examination.
- In the event of a Data Breach where there is an expectation of harm, Schoolbox will notify affected Customers without undue delay after becoming aware of the Data Breach. This notification will occur via email, to the registered technical and key contacts.
- When communicating a Data Breach we will include details of who is impacted, what is the potential impact and any steps we have taken to prevent further harm.
- Where applicable Schoolbox will notify the relevant regulatory authorities to report the breach.

Compliance

Schoolbox commissions third-party audits to measure the effectiveness of these technical and administrative controls against industry standard security frameworks.

Measures include:

- Schoolbox conducts regular internal audits of its security and expects to conduct external audits.
- Schoolbox has a formal policy for managing suppliers who have access to Personal Data and this includes criteria for reviewing and approving suppliers and procedures

for monitoring and reviewing their performance. Where appropriate suppliers may be required to sign a Data Processing Addendum.

- Schoolbox takes reasonable steps to ensure that Personnel are aware of and comply with the technical and organisational measures set forth in this document.
- Schoolbox conducts third-party penetration tests.