IT & Network Requirements

Technical specifications for school IT administrators deploying AchievoEDU.

All Plans | IT Administrator | Version 1.3

ABOUT THIS DOCUMENT

Intended for school IT coordinators and network administrators. Covers everything needed to whitelist, deploy, and support AchievoEDU across your school network.

1. Platform Overview

AchievoEDU is a cloud-based platform hosted on Microsoft Azure in Australia (Sydney). It is accessible via web browser on any device and via dedicated native apps on iOS and Android. There is no software to install on school-managed desktops or laptops.

Component	Details
Hosting provider	Microsoft Azure — Australia East (Sydney)
Data residency	100% Australia — all data stored and processed in Sydney. No international replication.
Platform type	Web application (SaaS) and native mobile apps — no desktop software required
Web access	Any modern browser at app.achievoedu.com.au
iOS app	AchievoEDU — available on the Apple App Store. Requires iOS 16 or later.
Android app	AchievoEDU — available on Google Play. Requires Android 10 or later.
Authentication	Email and password for all account types
Biometric login	Face ID / Touch ID supported on iOS app for returning users (device-level, not stored by AchievoEDU)
Encryption in transit	TLS 1.2 (minimum enforced). TLS 1.3 also supported. Cipher: AES-256-GCM
Encryption at rest	AES-256 via Azure Transparent Data Encryption (TDE) — enabled by default on all Azure SQL databases

2. Network Requirements

2.1 Firewall and Whitelist

The following domains must be permitted through your school firewall. All traffic uses HTTPS on port 443.

Domain	Purpose	Required?
achievoedu.com.au	Main website and login entry point	Yes
app.achievoedu.com.au	Web application — primary access point for staff and students	Yes

api.achievoedu.com.au	Backend API — required for all platform functions	Yes
*.azurefd.net	Azure Front Door CDN — static asset delivery	Yes
*.blob.core.windows.net	Azure Blob Storage — document and image hosting	Yes
*.applicationinsights.azure.com	Azure Application Insights — error and performance monitoring	Confirmed active

FILTERING AND PROXY NOTES

If your school uses SSL inspection (e.g. Cisco Umbrella, Fortinet, Smoothwall), exclude app.achievoedu.com.au and api.achievoedu.com.au from deep packet inspection. TLS interception on these endpoints will break authentication.

2.2 Mobile App Network Requirements

The native iOS and Android apps communicate with the same API endpoints as the web application. No additional domains need to be whitelisted for the mobile apps beyond the list above. Schools using Mobile Device Management (MDM) to manage student devices can allow-list the AchievoEDU app by its bundle ID:

Platform	App name	Bundle / Package ID	Store
iOS	AchievoEDU	com.achievo.school	Apple App Store
Android	AchievoEDU	com.achievo.school	Google Play Store

2.3 Ports and Protocols

Port	Protocol	Direction	Purpose
443	HTTPS / TLS 1.2+	Outbound	All web and API traffic
80	HTTP	Outbound	Redirect to HTTPS only — no data transmitted

2.4 Bandwidth Estimates

AchievoEDU is a lightweight application. The following are approximate estimates per concurrent user session:

Activity	Approximate bandwidth
Idle / dashboard view	< 10 KB/s
Awarding points / active use	< 50 KB/s
Loading reports or exports	< 200 KB/s (brief burst)
Recommended minimum per school	1 Mbps dedicated for up to 50 concurrent users

3. Browser Compatibility

AchievoEDU is tested against current versions of all major browsers. No minimum browser version is enforced, but browsers more than two major versions behind current release may experience degraded performance. The admin panel is fully functional on mobile browsers — there is no separate mobile admin interface.

Browser	Platform	Staff portal	Student portal	Admin panel
Google Chrome	Windows, macOS, Android	Recommended	Recommended	Recommended
Microsoft Edge	Windows, macOS	Supported	Supported	Supported
Mozilla Firefox	Windows, macOS	Supported	Supported	Supported
Apple Safari	macOS, iOS	Supported	Supported	Supported
Internet Explorer	Windows	Not supported	Not supported	Not supported

RECOMMENDATION
Google Chrome is recommended for all shared school devices. For managed iOS devices, Safari is the recommended browser. Internet Explorer is not supported.

4. Device Requirements

AchievoEDU runs in-browser with no local installation. Any device capable of running a supported browser can access the platform. The native iOS and Android apps are available as an alternative access method and are particularly suited to staff using personal or school-issued phones.

Device type	Access method	Requirements
Desktop / laptop (Windows)	Web browser	Any modern browser — Chrome, Edge, or Firefox recommended
Desktop / laptop (macOS)	Web browser	Any modern browser — Chrome or Safari recommended
iPad (managed)	Web browser or iOS app	iPadOS 16 or later
iPhone	iOS app or web browser	iOS 16 or later
Android phone or tablet	Android app or web browser	Android 10 or later
Chromebook	Web browser	Chrome browser — fully supported
Student BYOD phone	Web browser	Any current iOS or Android browser

5. Authentication and Identity

5.1 Current authentication

AchievoEDU currently uses email and password authentication for all account types. There is no multi-factor authentication (MFA) or Single Sign-On (SSO) at this time.

Account type	Login method	Password reset

Administrator	Email and password	Self-service on login page, or triggered by another administrator
Teacher / Staff	Email and password	Self-service on login page, or triggered by a school administrator
Student	Email and password	Self-service on login page, or triggered by teacher or administrator

5.2 Biometric login (iOS app)

The iOS app supports Face ID and Touch ID for returning users. Biometric authentication is handled entirely at the device level by Apple's framework — AchievoEDU does not store or transmit biometric data. Biometric login is not available in the web browser or Android app at this time.

5.3 Planned: SSO (2027 roadmap)

Support for Microsoft Entra ID (Azure AD) Single Sign-On and Google Workspace SSO is on the AchievoEDU development roadmap, currently planned for 2027. Schools with a strong SSO requirement should contact contact@achievoedu.com.au to register their interest and be notified when this feature becomes available.

5.4 Student account access

Student accounts use the student's school-issued email address and a password. Students do not need personal email addresses. This is intentional — it avoids the need to provision personal email accounts for primary-aged students and reduces the risk of account misuse.

FOR MDM ADMINISTRATORS

There are no device-level certificates, profiles, or MDM policies required to deploy AchievoEDU. The platform is entirely browser and app-store based. For managed iOS devices, the AchievoEDU app can be pushed via Apple School Manager.

6. Data and Privacy

Topic	Details
Data location	100% Australia — Microsoft Azure Australia East (Sydney). No international replication.
Data Processing Agreement	Completed DPA available — contact support@achievoedu.com.au to request a copy
Privacy Act compliance	Designed to comply with the Australian Privacy Act 1988 (Cth)
Student data use	Never used for advertising, profiling, or sold to third parties
Backups	Automated daily backups with 30-day retention, stored in-region
Data deletion	All school data permanently deleted within 30 days of written request or contract end
Security monitoring	Azure Application Insights used for error and performance monitoring (no personal data processed)

7. Support and Contacts

Contact type	Details
Technical support email	support@achievoedu.com.au
Platform status page	status.achievoedu.com.au — live status and incident history
Support hours	Monday to Friday, 8:00am to 5:00pm AEST
Onboarding enquiries	achievoedu.com.au/contact or contact@achievoedu.com.au
App Store (iOS)	Search 'AchievoEDU' on the Apple App Store
Google Play (Android)	Search 'AchievoEDU' on Google Play