



A product of



ClassPilot Security and Data Protection Overview

Version 0.2 | 19 September 2026

This overview supports a school's supplier checks. It describes the ClassPilot security design and shared responsibilities. It is not a certification, penetration-test report or guarantee of uninterrupted service. The final issued version must match verified production controls.

1 Service and data boundaries

ClassPilot is an assessment and reporting service supplied by Edapt Technologies. Schools control their educational records; the Data Processing Agreement sets out our processor obligations. The privacy notice explains our limited separate controller activities.

Core application and database resources have been configured in Microsoft Azure UK South. All requests have a separate processing route whose geography and retention must be verified. This overview does not claim that every supplier activity takes place exclusively in the United Kingdom.

2 Access and school separation

The application design uses invited accounts, authenticated sessions and school, role and class scopes. Authorisation is enforced on the server for protected operations. A shared database does not mean schools are permitted to view each other's records.

Microsoft work-account sign-in, where configured, identifies the user but does not grant unrestricted product access. The school must authorise the account and its permissions. Schools should use appropriate identity-provider security, including multifactor authentication where available; this is not a claim that ClassPilot enforces MFA for every sign-in route.

3 Connections and privileged access

The design uses HTTPS for application connections, SSL-required database connections and Azure platform encryption for supported stored data. Production secrets are held in protected configuration or Azure Key Vault rather than being published in source code.

Edapt access to school information must be limited to authorised people who need it for an agreed support, security or operational purpose. Relevant access must be protected by confidentiality duties. Schools must never provide staff passwords to support.

4 Logging development and recovery

Relevant authentication, administration, record-change and reporting events are recorded where supported. Logs should avoid unnecessary pupil content. Their coverage, access restrictions and retention must be verified for the production release.

Source control, dependency review, automated tests and controlled releases support development assurance. School isolation and role permissions require explicit testing. Passing functional tests is not equivalent to an independent security assessment.

Azure backup capabilities support recovery, but the configured schedule, maximum retention and a successful restore test must be recorded before live onboarding. No specific recovery time, recovery point or availability percentage is promised by this draft. The Order Form must state any separately agreed service levels.

5 Suppliers and incidents

The current draft DPA identifies Microsoft Azure and Azure OpenAI. The complete supplier list must also account for any email delivery, support mailbox, monitoring or other provider that handles school personal data. A school must receive the completed subprocessor schedule before its data is processed.

Report suspected exposure or unauthorised access promptly to support@edapt-tech.co.uk with the subject Urgent Security Incident. Provide the time, affected function and a minimal description; agree a secure route before sending sensitive evidence. Edapt will investigate and notify the controller without undue delay after becoming aware of a personal-data breach. The DPA governs notification duties.

6 What the school must do

- Approve users and access scopes, remove leavers promptly, and secure devices, networks and Microsoft or other identity accounts.
- Approve the lawful use of pupil data and AI, provide appropriate privacy information, and involve the school's data protection lead.
- Check imported data, review reports and protect exported files. Follow the Acceptable Use Policy and agreed secure transfer arrangements.

7 Evidence and review

Schools may request proportionate assurance information through support@edapt-tech.co.uk, including data flows, verified backup details, testing summaries and information to support a DPIA. Detailed technical material may be supplied privately where disclosure would create a security risk.

This draft makes no claim of ISO 27001 certification, Cyber Essentials certification, completed independent penetration testing or a completed accessibility audit of the live application. Any future assurance claim must identify its scope, date and evidence. Outstanding checks must be resolved before this document is issued as a statement of live controls.