Security overview for schools

Version 2026-09-30 v1 · Last updated 30 September 2026

Wilgenry Software Limited (trading as Squono), a company registered in England and Wales, company number 17392061, registered office 42a Church Street, Hatfield, England, AL9 5AW. Email hello@squono.com.

What Squono actually does to protect school data, and what it doesn't do yet. This is the security annex to the data processing agreement.

Hosting and network

- Hosted on AWS Lightsail in London (eu-west-2), behind nginx. The app itself listens only on the server's internal address.
- The server firewall is open only on ports 22 (SSH), 80 and 443.
- Squono's services run as an unprivileged system user, not as root.
- Photos and documents are in object storage in London; email goes through Amazon SES in London.

Encryption

- HTTPS everywhere (TLS 1.2 and 1.3 only), with HTTP Strict Transport Security (one year, including subdomains).
- A Content Security Policy that stops other sites framing Squono (frame-ancestors none) and allows scripts only from Squono itself and Google's gstatic.com, which serves the Google Cast loader on match video pages. Schools don't use match video.
- Field-level AES-256-GCM encryption for the few secrets Squono holds, such as API tokens and volunteer bank details.
- Invitation, share and payment link tokens are stored only as SHA-256 hashes.

Encryption at rest – where things stand

- The database and files are on AWS in London.
- Squono does not yet add its own encryption layer to the database server's disk or to the backup files on the server. Those backups are files readable only by the server's root user, on the same server, kept for 14 days. Encrypted off-site backups are planned.
- Photos and documents are in AWS object storage in London, which encrypts every stored file at rest by default (AES-256, keys managed by AWS).

Accounts and sign-in

- Passwords are hashed with scrypt. Email addresses must be verified.
- Two-factor authentication (an authenticator app, TOTP) is mandatory for every school staff account – administrators, office staff, teachers and visiting coaches – before they can see any school data. This is enforced in the server's permission layer, not just the screens.
- Two-factor authentication is optional for parents, and always required for Squono's own platform administrators.
- Sessions last 30 days. Cookies are httpOnly, secure and SameSite=Lax.
- Rate limits on sign-in, one-time codes and two-factor attempts.

Access control

- Every request is permission-checked on the server. Each team is a separate boundary, then audience rules decide who sees each item; restricted items are for staff only.
- Parents see only their own children and those children's teams. Pupils have no accounts.
- Data a person isn't allowed to see is never sent to their browser or phone.
- Squono staff can see a school's data only through a support grant the school approves: 2 hours by default, 24 hours at most. Every access is recorded in the audit log.

Logging

- An audit log records administrative, sharing, publishing and deletion actions. It never contains children's names or message text.
- IP addresses in audit and activity logs are stored only as keyed hashes (HMAC-SHA256).
- Sign-in session records do hold the IP address and browser used, until 1 day after the session expires.

Photos

- Location and other EXIF data is removed from photos before upload in the web and mobile apps.
- The server also checks JPEG, PNG and WebP uploads for leftover GPS data.
- Photos are private to the people the school chooses and are served through permission-checked links. There is no face recognition.

Backups and recovery

- Daily database backups, kept for 14 days on the server, plus the hosting provider's snapshots. All backups roll off within 35 days.
- Squono's written backup procedure covers restoring to a new database and re-applying deletions made since the backup, and requires a restore test at least every quarter.
- Squono is a free service and doesn't offer a contractual availability (uptime) guarantee.

Certifications and testing

- Cyber Essentials: not yet certified.
- ISO 27001: not certified.
- Penetration test: none yet. One is planned.
- No full accessibility audit yet either (see the accessibility statement).

Keeping software up to date

Dependencies are updated regularly. Squono doesn't claim a fixed patching deadline, but aims to meet the Department for Education's cyber security standard for schools, which expects critical and high-risk patches to be applied within 14 days.

Incidents and breaches

If a personal data breach affects school data, Squono tells the school without undue delay – with a target of 24 hours and never later than 48 hours after becoming aware of it – as set out in the DPA (squono.com/schools/trust/dpa), section 13.

What Squono doesn't do

- No analytics, tracking or advertising tools.
- No third-party scripts, apart from the Google Cast loader on match video pages (not used by schools).
- No selling or sharing of data for anyone else's purposes.