

Handing over pupil and staff data to a new supplier is a big responsibility, and we know data protection is often the first thing a school's DPL or SLT wants reassurance on. This document summarises how we approach data protection and security day-to-day. It sits alongside our full [Data Protection Policy](#), [Data Processing Agreement](#) and [privacy policy](#).

Data protection isn't a box we tick once a year - it's built into how we run the business every day. If you have questions this summary doesn't answer, we're happy to talk them through.

1. We meet all legal requirements

Quest Assessments complies with the UK GDPR and the Data Protection Act 2018, and follows the ICO's Age Appropriate Design Code throughout the platform. We hold Cyber Security Essentials certification. Your school is the Data Controller for pupil and staff data; we act as your Data Processor, processing data only in line with your instructions and our Data Processing Agreement.

2. We train our team, continuously

All Quest employees complete mandatory Cyber Security and Data Protection training, with enhanced training and refresher courses for anyone who regularly handles personal data. Our engineers also complete code security training, and our security policies are formally reviewed every year to reflect changes in the law and in best practice.

3. We collect only the data we need

We deliberately limit what we ask schools for. For Quest Progress, this means a pupil's full name, date of birth (needed for age-based scoring), ESOL status, and a single-letter SEN provision code (N/S/E/K) - we don't hold any further detail about a pupil's SEN history or needs. We don't use Large Language Models (AI) anywhere in the platform, and the only automated processing of personal data is age- and month-of-birth-based scoring, so pupils are assessed fairly against others in their year group. Even our machine learning scoring works from anonymised data referenced only by an identifier. No pupil names or personal details are used.

4. We have robust safeguards in place to protect your data

Security isn't a single control - it's layered through our infrastructure, our access controls, our testing and our people.

Infrastructure & resilience

- Cloud-hosted across Google Cloud Platform and Digital Ocean, with data centres in London and Belgium, and Cloudflare for DNS, load balancing and firewall protection.
- Built for resilience, with automatic failover and standby nodes on every data store, and a database technology that's resilient by design.
- Every outage or near-miss is investigated to improve resilience going forward.

Access control & authentication

- Every account is unique and authenticated via encrypted, regularly-expiring tokens, with faster expiry for admin accounts.
- Multi-factor authentication is available on every account and can be enforced for specific users or schools.
- Internally, we enforce single sign-on and 2-step verification, and give staff only the access their role requires.

Encryption

- All data in transit is encrypted via HTTPS/TLS, and all customer data is encrypted at rest.
- Internal traffic runs over isolated, encrypted networks rather than the open internet.
- Passwords are never stored in plain text. They're one-way hashed with a unique salt per user.

Testing & assurance

- We release weekly, with automated and manual testing, a pre-production environment mirroring live, and gradual, canary rollouts.
- We run an annual independent penetration test, alongside ongoing internal testing of sensitive features before release.

People & physical security

- All staff undergo background checks, including Enhanced DBS for anyone in regular contact with pupils, and have access revoked on leaving.
- We run continuous threat monitoring, with remote lock or wipe for suspicious device activity.
- Our London office uses key-card access, CCTV, and secure, restricted storage.

5. If something does go wrong, we're there to support you

We understand what's at stake for your pupils and your school, so every incident or near-miss is logged, investigated and acted on. If a breach affecting your data were to occur, we would notify you immediately and work with you on investigation, mitigation and any reporting to the ICO. Our data protection team is always reachable directly at gdpr@questassessments.com.