Quest Data protection and security summary

This document summarises the Quest data protection, privacy and security policies. It sits alongside the full Data Protection Policy, Data Processing Agreement and privacy policy.

Data protection is not just a box we tick once a year. It's fundamental to how we run Quest.

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. Quest only processes data 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. All staff undergo background checks, including **Enhanced DBS** for anyone in regular contact with pupils, and have access revoked on leaving.

3. We collect only the data we need

We deliberately limit what we ask schools for. The only automated processing of personal data is age, which is used for scoring, ensuring pupils are assessed fairly against others in their year group. The scoring works from **anonymised data,** referenced only by an identifier. No pupil names or personal details are accessible.

4. We have robust safeguards to protect your data

Safeguards are layered throughout the Quest infrastructure, access controls, and our people.

Infrastructure

- Cloud-hosted across Google Cloud Platform and Digital Ocean, with data centres in London and Belgium, meaning we’re not reliant on any one data centre.
- Automatic failover on every data store, so if something does go wrong, there’s a back-up ready.

Access control

- Every account is unique and authenticated via encrypted, regularly-expiring tokens.
- Multi-factor authentication is available on every account.
- Our people only have the access their role requires.

Encryption

- All customer data is encrypted and passwords are never stored in plain text.
- Internal traffic runs over isolated, encrypted networks.

Testing

- All technical changes go through both automated and manual testing, before being released gradually to customers.
- We run an annual penetration test where we hire an independent company who attempts to access our data, ensuring our security measures are tried and tested.

Physical security

- We run continuous threat monitoring, with remote lock or wipe for suspicious device activity.
- Our physical office uses key-card access, CCTV, and secure, restricted storage.

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

We know what's at stake for your pupils and your school. 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.