

THE SHORT VERSION

Quilva is designed so the core authorship process happens locally, offline and under the school's control. The application does not upload student essays to Quilva for analysis, and the Quilva website does not need access to the student's project files.

1 WHERE IS STUDENT DATA STORED?

On the school's device/storage. Quilva's project is a self-contained .qlv file. The documentation describes the project as portable and local: manuscript text, planning data and the authorship evidence are held in the project on the user's machine.

Quilva does not operate a cloud workspace for student essays. The school controls where project files are saved, backed up and deleted.

2 WHAT DOES THE AUTHORSHIP ENGINE DO?

The Human Authorship Certificate is generated by the desktop application. Quilva records behavioural/process evidence such as keystrokes, pasted/imported text, deletions and working time. The documentation states that this notebook remains inside the project file and that the detection itself is entirely local.

3 DOES THE WEBSITE SEE THE ESSAY?

Not for normal offline analysis. The website is not where the authorship decision is made. Quilva's desktop application performs the local processing.

QR verification is a separate, optional step. A certificate contains an encrypted, compressed summary and a small selection of manuscript sentences. When somebody scans it, that encrypted payload can be sent to quilva.com so the server can decrypt and display the certificate readout. The documentation states that the payload is not retained after display.

4 ENCRYPTION & TAMPER RESISTANCE

The certificate seal is encrypted and bound to the project file. The documentation describes PBKDF2-derived key material and AES-256 stream encryption. Editing or moving the seal between projects causes certificate generation to lock for the affected file.

THE NETWORK BOUNDARY — WHAT ACTUALLY NEEDS THE INTERNET?

ACTIVITY	NETWORK REQUIRED?	WHAT LEAVES THE MACHINE?
Writing / editing	NO	Nothing is uploaded for authorship analysis.
Human-authorship analysis	NO	Processing is performed by the desktop application.
Licence activation / validation	LICENSING STEP	Only the licensing information required by the licence system.
QR certificate verification	OPTIONAL WEB STEP	Encrypted certificate payload + selected snippets, so the server can decrypt/display the readout.

5 DATA PROTECTION: WHAT THIS MEANS FOR A SCHOOL

DfE guidance says schools must protect personal data, document compliance, maintain appropriate policies and consider DPIAs where processing is likely to create high risk. DfE also advises caution around sharing children's data with third parties.

Quilva's architecture reduces the data-sharing surface: student work can remain within the school's managed estate rather than being uploaded to an external AI-analysis service.

DPIA: the school should assess Quilva in its own context and record the actual processing, retention, access controls and deployment model. Because Quilva can operate offline, the data flow is unusually straightforward to document.

DPA: whether a formal processor agreement is required depends on what personal data the school asks Quilva Ltd to process. Normal offline authorship analysis does not require Quilva's servers to receive the student's manuscript.

6 INSTALLATION & SECURITY

Windows: standard install wizard. Linux: self-contained executable. macOS: portable application folder. Quilva is designed as a self-contained desktop application rather than a browser/cloud service.

No cloud dependency for writing. The school can install Quilva on managed student machines and keep project files within existing school storage, permissions, backups and device-management controls.

Antivirus: Quilva's documentation notes that some scanners may flag the local authorship component on first run. This is described as a false positive; nothing is transmitted by the component. IT can verify the installer and apply its normal software allow-list process.

Windows signing: Quilva Ltd states that its Windows software is code-signed using SSL.com credentials for QUILVA LTD. As with any third-party software, schools should apply their normal endpoint-security verification and deployment policy.

THE IT TEST

Want to verify the architecture yourself? Install Quilva on a test machine, disconnect/block its internet access, create a project and write normally. The local authorship workflow remains local. The specific online/licensing or optional certificate-verification steps are separate.

OPERATING SYSTEMS	Windows • macOS • Linux	PROJECT STORAGE	Local .qlv project file
CORE ANALYSIS	On-device / offline	CLOUD ESSAY STORAGE	None for normal offline operation
DATA CONTROL	School/device administrator controls storage & access	CERTIFICATE	Encrypted QR payload; optional web verification

Important procurement note: This brief describes Quilva's published technical architecture and intended operation; it is not legal advice and does not replace a school's own DPIA, privacy notice, information-security assessment or procurement checks. Schools should confirm the precise licence/support arrangements and current software version with Quilva Ltd before deployment.

Sources: quilva.com • quilva.com/docs.html • quilva.com/schools.php • Department for Education, "Data protection in schools" (updated 9 July 2026) • DfE school technology/data-protection guidance. | Prepared September 2026.