Pavryn

Information security statement

Version 1, in effect from 19 November 2026.

How Pavryn Learn is built and run, as at 19 November 2026. This describes what is in place.

Where it runs

- Pavryn Learn runs on Microsoft Azure in the UK South region, and its database is in the same region.
- The database is held in the Azure Databricks service, which we buy from Microsoft under Microsoft's terms.
- **One exception to UK hosting: the policy check.** When someone uses it, the policy they give it and the text of the course they choose are sent to Anthropic, which provides the AI model, in the United States. Anthropic's terms do not allow it to use them to train its models. Nothing is sent unless someone uses the check.

Keeping each council's records apart

- Every record belongs to one council.
- The separation is enforced twice: by the application, and again by the database itself, which refuses to return or change another council's rows even if a query is wrong.
- The account the running service uses to reach the database cannot change the database's structure, create a council or give anyone access to one.
- A person sees a council's records only if they have been given membership of that council. A Microsoft account alone is not enough, and a council's Microsoft directory must be admitted before any of its accounts can be used.

Signing in

- The usual way to sign in is the person's Microsoft work account, so your council's own sign-in rules apply, including multi-factor authentication where you require it.
- Pavryn Learn stores no passwords. Signing in with a password is switched off.
- Sign-in cookies are sent only over HTTPS, cannot be read by scripts in the page and belong to app.pavryn.com alone.
- When someone's access is withdrawn, it takes effect at their next request.
- Repeated sign-in requests are counted and limited.

In transit and in storage

- All traffic uses HTTPS, with certificates managed by Azure.
- File storage accepts only TLS 1.2 or later and refuses anonymous access and shared keys. Every container is private.
- The database is encrypted at rest by the Azure Databricks service that holds it.

- Azure Storage encrypts stored files at rest.

Secrets and the service’s own access

- The service’s secrets are kept in Azure Key Vault and read by the running service through its own Azure identity. None is kept in the code or in the images.
- That identity can read the published course files and its own secrets. It is given no right to write to either.
- The image registry is private and its administrator sign-in is disabled. The containers run as an unprivileged user.
- Key Vault keeps a deleted secret recoverable for 90 days and does not allow it to be purged early.

In the browser

- Pavryn Learn checks that each request that changes something came from its own pages, and limits the size of requests.
- It sets cookies only to sign people in and keep them signed in and, in a demonstration, to open it and to keep a visitor’s own changes for their visit.
- Our website sets no cookies, loads nothing from third parties and sends a content security policy.

Records and logs

- Pavryn Learn keeps its own record of changes to a council’s settings: when, who and what.
- It records each certificate’s reference and each time one is downloaded, and by whom.
- Application and platform logs go to an Azure Log Analytics workspace in our own subscription and are kept for 30 days.

Backups and recovery

- The database keeps seven days of history, so it can be put back to an earlier point within that time.
- When a record is deleted, that history keeps it for up to seven more days.
- Course files are versioned, and a deleted file can be recovered for 30 days.

How changes are made

- Every change is kept in version control and runs automated tests before release. The tests cover the database’s rules, including the separation between councils, the pages, and accessibility scans.
- The service is built from pinned base images and a locked list of dependencies.
- Each release is checked against a written list before it goes live, and the record of the check is kept.

If something goes wrong

- If we become aware of a personal data breach that affects your council’s records, we will tell you without undue delay, with what we know, so that you can meet your own duties.
- To report a security concern, email data@pavryn.com.

When a contract ends

- **A copy on request.** We give the council a full copy of its records in open formats within 10 working days of being asked, once, at no charge.
- **30 days to collect.** For 30 days after the end date the council's administrators can still sign in and download. Nothing can be assigned or changed.
- **Deletion.** We delete the council and all its records within 30 days after that, or sooner if the council asks in writing.
- **Backups and logs.** Backup history clears within 7 further days, and logs within 30.
- **Confirmation.** We confirm the deletion in writing, with its date.
- **What we keep.** The contract, invoices and correspondence, for six years, and the fact that the council was deleted and when. Nothing about its people.

The suppliers that process a council's data for us are named in our privacy notice at pavryn.com/privacy.

Pavryn Ltd, registered in England and Wales, company number 17483267. Registered office: 1 Broughton Close, Taunton, TA1 2JS. Registered with the Information Commission's Office (ICO), reference ZC259046.