Trust & Security

Feaniks HQ — Workforce Intelligence for Health and Care

Version v2.6.1

November 2026

Feaniks Ltd · 167-169 Great Portland Street, Fifth Floor, London W1W 5PF

Registered in England & Wales · Company No. 12109594

Last updated: 10 November 2026 (v2.6.1)

Feaniks builds workforce competency and training-evidence software for UK health and care organisations. This page documents how we protect the data our customers entrust to us, what obligations we take on as a processor, and where our infrastructure lives.

If you're doing due diligence during a procurement conversation, everything you need should be here. If it isn't, email security@feaniks.com — we'll answer directly, not through a portal.

Where your data lives

Application data — UK only. Everything about your staff, their competency evidence, their training records, their supervisions, observations, feedback, and assessments — the operational heart of Feaniks HQ — is stored in the United Kingdom on Google Cloud Platform's `europe-west2` region (London).

This is not a preference. It is a hard-coded position enforced by our infrastructure controls. We do not operate any HQ infrastructure outside the UK, and we do not use any UK data for training AI models, product analytics, or any purpose beyond delivering the service you contracted for.

Online training — UK. Online training will run through Feaniks HQ's own course player, being built on the same UK infrastructure. No separate learning platform or sub-processor is involved.

Customer end-user identity — UK. Organisations without their own Microsoft sign-in will use a Feaniks-hosted Microsoft Entra External ID tenant (`feaniksid.onmicrosoft.com`, UK South), with MFA enforced by Feaniks before it goes live. This tenant will hold sign-in metadata only — email address, MFA registration state, session tokens — and will never receive operational data. Where your organisation federates its own identity provider instead (see Multi-factor authentication, below), no end-user credentials touch Feaniks infrastructure at all.

Feaniks staff identity — EMEA. Feaniks' own staff authenticate through our Microsoft Entra ID business tenant. Microsoft hosts Entra ID identity data in EMEA. This tenant is staff-only; no customer data flows to it.

Multi-factor authentication

MFA is not a single control — it depends on who is signing in.

Feaniks' own staff (internal engineers, support, operations). Enforced via Microsoft Entra Security Defaults on the Feaniks Ltd business tenant, using the Microsoft Authenticator app. SMS and voice-based MFA are disabled. Every Feaniks staff member accessing customer systems has MFA enforced with no exceptions. Verified on 4 August 2026, with evidence retained.

Your organisation's own staff. MFA is enforced by your organisation's identity provider. Feaniks does not override or weaken your controls. If your DSPT self-assessment commits your organisation to MFA on all cloud services, our authentication pattern makes that commitment straightforward to

honour — your IdP's policy flows through into Feaniks HQ automatically, without any separate Feaniks-specific configuration on your side.

Why we don't run in-app "Feaniks MFA" as a separate layer. Some products in adjacent categories issue their own TOTP/OTP challenge in addition to your organisation's login. We deliberately don't. Adding a second product-controlled MFA layer on top of an IdP-enforced one does not increase security materially; it does add credential management overhead, recovery-flow complexity, and one more thing that can break at 2am when a manager needs urgent access. We may revisit this position if a specific customer requirement or a regulatory change makes it warranted.

Audit logging

Sign-in activity, sign-out activity, and rate-limit events are logged with actor, timestamp, source IP, and action type. The audit log is append-only at the database level (enforced by a row-level trigger) and retained for a minimum of 12 months.

Roadmapped. Broader audit coverage across create, update, and delete operations on staff records, competency evidence, training records, supervisions, observations, and assessments will be added as those parts of Feaniks HQ are completed. Where a customer contract or regulator requires broader audit coverage today, tell us — we will scope the specific coverage needed against your timeline.

Access to audit logs. Your organisation's Feaniks HQ administrators can request audit log extracts about their own tenant via support. Feaniks staff access audit logs only when investigating a specific support ticket or security incident, and access is limited to named Feaniks staff and recorded in the support ticket.

Encryption

In transit: TLS 1.2+ enforced on every endpoint. Older TLS versions and cipher suites are actively rejected.

At rest: AES-256 encryption on all data stores, using Google-managed encryption keys.

Between services: All inter-service communication inside our infrastructure is over encrypted channels; nothing sensitive travels over cleartext internal networks.

Passwords and secrets: Never stored by Feaniks in plaintext. Where Feaniks stores credentials for third-party integrations (for example, connections to your organisation's own systems), they are held in Google Cloud Secret Manager with strict IAM-restricted access.

Data Security and Protection Toolkit (DSPT)

These references use the care-provider DSPT numbering; we will map them to the CAF-aligned outcomes your IG team uses. DSPT 4.5.3 requires health and social care organisations to enforce MFA on cloud services their staff use. This is your organisation's obligation as the data controller, not Feaniks' obligation as processor.

How Feaniks helps you meet 4.5.3: Because your staff authenticate through your own IdP (or, once it is live, through the Feaniks-hosted Entra External ID tenant with MFA enforced by Feaniks), your existing MFA enforcement flows through into Feaniks HQ automatically. You do not need to configure a separate Feaniks-specific MFA policy. This design choice helps you answer DSPT 4.5.3 for Feaniks HQ without additional work on your part.

DSPT 4.4.1 least privilege — how the tenant-privileges split helps. DSPT 4.4.1 asks that access rights be granted on a least-privilege basis. Our three independent tenant privileges (below) let you separate administrative, reporting, and billing responsibilities without granting a single super-user role — a finance controller can hold Billing without Admin or Reporting, a compliance lead can hold Reporting without Admin.

Feaniks' own DSPT position. Feaniks is below the size threshold for the DSPT 'IT Supplier' organisation type. Where we process personal data for an NHS organisation, we will complete and publish a Data Security and Protection Toolkit assessment under the appropriate organisation type before any NHS data is processed.

Three independent tenant privileges

Feaniks HQ separates tenant administration into three privileges that can be granted independently to any user, alongside their operational role. This exists both for UK GDPR data-minimisation and for DSPT 4.4.1 least privilege.

- **Admin privileges** — the tenant administration surface: invite users, assign roles, structure the Organisation, manage integrations.
- **Reporting privileges** — the reporting and export surface: CSV exports, Board Pack, audit log extracts, competency evidence packs.
- **Billing privileges** — buy credits (which set the online courses available to your staff), buy additional Feaniks HQ Licences, one-time tier selection, view invoices, update payment method.

The Owner holds all three by default. Any privilege can be granted independently to any user without granting the others. A finance controller can be given Billing without ever seeing operational data. A compliance lead can be given Reporting without administrative rights.

Two lockout safeguards. The Owner's three privileges are protected — any attempt to remove them is refused by any administrator, and only an Owner transfer ceremony can remove them. Separately,

a non-Owner administrator cannot remove their own Admin privileges (self-revoke is forbidden for Admin, to prevent an accidental lockout); Reporting and Billing self-revoke is unrestricted.

What Feaniks does as a processor

Under UK GDPR, your organisation is the data controller for the personal data you put into Feaniks HQ (your staff's records, the people you support (residents or patients) referenced in incidental context, and so on). Feaniks is the data processor.

Our processor obligations, in specifics:

- We process personal data only on your documented instructions (your subscription, your DPA, your configured integrations). We do not use your data for our own purposes.
- We do not sell, rent, or share your data with any third party except the specifically-listed sub-processors below, and only to the extent required to deliver the service.
- We notify you without undue delay of any personal data breach affecting your data — our target is within 24 hours of Feaniks becoming aware, and always well within the 72-hour statutory window your organisation would need to notify the ICO.
- We assist you with data subject rights requests (access, rectification, erasure) when the data subject is your staff member or is otherwise in your controller relationship.
- On contract termination, we return or delete your data on your instructions, within the timelines set in the DPA — with one specific carve-out described below for training records.
- **We do not use your data to train AI models across customers.** Any analytics or suggestions run only on your organisation's own data, for your use — never against pooled multi-customer data.

Our sub-processors:

- **Google Cloud (Google LLC / Google Cloud EMEA Limited)** — UK infrastructure (`europe-west2`) for application data, databases, and file storage.
- **Microsoft Corporation (Entra ID — Feaniks Ltd business tenant)** — identity services for Feaniks staff sign-in, hosted in EMEA. No customer application data flows here.
- **Microsoft Corporation (Entra External ID — `feaniksid` tenant)** — customer end-user identity for the Feaniks-hosted sign-in route, UK South, for organisations without their own Microsoft sign-in. It will hold email address, MFA state, and session tokens only; no operational data.
- **HighLevel, Inc. (GoHighLevel / LeadConnector)** — customer engagement platform and portable learner registry, US-hosted. Transfers rely on HighLevel's certification under the UK Extension to the EU–US Data Privacy Framework (the UK–US data bridge). HighLevel holds learner names and email addresses for these purposes only; it holds no staff records, Moments, evidence or information about the people you support. This is the only sub-processor that holds customer personal data outside the UK, and it does so for a specific, limited purpose (engagement communications and the portable training-record registry).

We give you 30 days' notice of any change to the sub-processor list.

Training-record retention after contract termination

Care workers move between employers, and their training investment routinely gets lost each time they do — new employer, new onboarding, retrain from scratch. Feaniks HQ addresses this with a portable training-record layer.

On contract termination, Feaniks retains training records for 7 years at no additional cost. Where your organisation's own retention schedule requires longer (for example, the NHS Records Management Code of Practice recommends ten years for statutory and mandatory training records), tell us and we will agree the retention period with you. The retained data is narrow: course completed, completion date, certificate reference, learner identifier. Operational records inside your Feaniks HQ tenant — competency evidence, supervisions, observations, assessments, staff notes — are returned or deleted per the DPA. Only the training-record layer is retained.

What "portable" means. Portable applies to training records only. It does not apply to competency evidence, assessments, observations, supervisions, feedback, or manager notes — those belong to the employer who recorded them and do not transfer.

How a transfer actually happens. Care worker asks a new employer to import their record. Feaniks contacts the previous employer with the specific list. Previous employer approves or declines. On approval, records are added to the new employer's Feaniks HQ tenant. The previous employer's approval is the release gate; a learner's request alone is not sufficient, because the previous employer paid for the training.

Lawful basis. UK GDPR Article 6(1)(f) legitimate interests — workforce competency portability serves the sector, workers, and employers. Learners are told at onboarding, through a privacy notice, that their training record is held in the engagement registry for potential future transfer, and they can object at any time via privacy@feaniks.com. On objection, name, email, and Feaniks identifiers are removed within 30 days, and training completion events are retained in anonymised form linked to the paying employer, not the learner, as evidence of that employer's training expenditure.

Roles and access inside your organisation

Feaniks HQ supports role-based access control. Your organisation's Feaniks HQ administrator (Owner role) controls who inside your organisation sees what.

Operational roles:

- **Owner** — full access to configuration, users, roles, and all data within your organisation's tenant. Holds all three tenant privileges (Admin, Reporting, Billing) by default.
- **Regional** — access across a defined set of services / regions within your organisation.
- **Service Manager** — access to staff records, competency evidence, and training data for their assigned service.

- **Team Lead** — access to staff records and competency evidence for their assigned team, including approval of competency evidence.
- **Staff** — access to their own competency and training data.

Any of the three tenant privileges (Admin, Reporting, Billing) can be granted to any of these roles independently. Your Owner can revoke any role instantly, and role changes are captured in the audit log.

Roadmapped. External-auditor and external-partner access (for CQC inspectors, freelance supervisors, external assessors) will be added when the first customer contractually requires it. When that happens, external users will authenticate through a dedicated Microsoft Entra External ID tenant with passkey-first MFA, and their read and write actions will be captured in a distinct external-role audit stream. If this is on your requirements list today, tell us — we can prioritise it in the roadmap.

Interim stopgap. Where a specific one-off external auditor needs access to your Feaniks HQ tenant ahead of the roadmapped track, we can invite them via Microsoft B2B guest collaboration on Feaniks' business tenant. This is a bridge, not a strategic answer, and comes with three honest caveats: the auditor's MFA depends on their own home tenant (which for a freelance inspector may not enforce MFA at all); guest audit entries are harder to segment from internal-user audit; the sign-in experience shows Feaniks branding rather than yours. Tell us and we'll walk through whether the bridge fits your scenario.

What we don't do

- **We do not provide clinical care planning.** Feaniks HQ is a staff-and-competency system, not a Person Record System. If the person you support (resident or patient) is referenced in a supervision or observation record, it is incidental — the record's subject is your staff member, not the person you support.
- **We do not offer SMS or voice MFA.** We use authenticator-app MFA only, as a deliberate security decision.
- **We do not run our own identity provider for your staff by default.** Where your organisation federates its own IdP, that IdP is the source of truth.
- **We do not train AI models on your data across customers.**
- **We do not pool customer data for cross-tenant analytics.** Where a customer wishes to opt into an anonymised benchmark, that will be an explicit opt-in, not a default.

Reporting a security concern

If you believe you have discovered a security issue affecting Feaniks or a customer using Feaniks, contact security@feaniks.com directly. We respond within one business day.

We do not currently operate a public bug bounty programme. We do accept responsible disclosure reports and will acknowledge every substantive report in writing.

Certifications and assurance

Feaniks does not currently hold ISO 27001, SOC 2, or Cyber Essentials Plus certifications. We treat these as commitments to make honestly rather than logos to display, and we will pursue certification when our scale and the specific requirements of our customer base make it appropriate.

Feaniks has not yet completed a Digital Technology Assessment Criteria (DTAC) assessment. We will complete the current DTAC (version 2.0) before Feaniks HQ is used within an NHS organisation.

If your procurement process requires evidence in the shape of one of these standards, contact us and we will discuss what equivalent assurance we can provide today.

Change history

- **10 November 2026 (v2.6.1)** — Corrected claims to match what is built today: the course player and the Feaniks-hosted sign-in tenant are described as in progress; encryption at rest uses Google-managed keys; Feaniks staff access to audit logs is recorded in the support ticket; analytics wording simplified. Clarified the HighLevel transfer mechanism and the data it holds, and the lawful basis for the learner registry (legitimate interests, with a privacy notice). Added a note on DSPT numbering, removed the trial reference, and widened the subtitle to health and care.
- **10 November 2026 (v2.6)** — Revised for NHS information governance review. Replaced the DSPT position with a commitment to complete and publish a DSPT assessment before any NHS data is processed. Added the DTAC position and a commitment to complete DTAC version 2.0 before use within an NHS organisation. Corrected the training-record retention wording against the NHS Records Management Code of Practice. Widened the scope to health and care organisations, aligned the Google Cloud entity with the Data Processing Addendum v1.1, and removed internal project references.
- **10 November 2026 (v2.5)** — Online training will run through Feaniks HQ's own course player, being built on the same UK infrastructure as the rest of Feaniks HQ. Removed the third-party learning platform from the sub-processor list, and updated the data-location and billing wording to match: staff are added to Feaniks HQ, and credits set the online courses available to them.
- **5 August 2026 (v2.4)** — Added Billing as a third independent tenant privilege alongside Admin and Reporting, with the two lockout safeguards (Owner protection, self-revoke forbidden for Admin). Added the 7-year training-record retention commitment after contract termination. Added the training-record portability section. Expanded the sub-processor list with the Entra External ID and HighLevel entries. Added no-cross-customer AI training as an explicit undertaking. DSPT section extended with a 4.4.1 least-privilege paragraph tied to the new tenant-privileges split.
- **4 August 2026 (v2.0)** — Revised to match the shipped state of Feaniks HQ. Removed forward-looking claims about a dedicated Entra External ID tenant, passkey-first MFA for external partners, an Inspector Portal, and broad create/update/delete audit coverage — all of which are

on the roadmap but not built today. Reframed those items as customer-triggered roadmap items. Corrected the roles list to match the shipped `HqMembershipRole` enum. Audit-logging section scoped to what the shipped audit log actually captures.

- **30 July 2026 (v1.1)** — Corrected a sub-processor description to make clear that customers contract with Feaniks Ltd, and that Feaniks Ltd is responsible to the customer for its sub-processors.
- **30 July 2026 (v1.0)** — First drafted.

For the definitive commercial terms, see your Master Subscription Agreement and Data Processing Addendum. Nothing on this page overrides those documents.