

Security Pack

WhealBit, trading as QWTN

October 2026

How QWTN protects customer records: hosting, access, audit, incident response and the answers to common security questions.

Ireland

Customer records stored on AWS, in the eu-west-1 region

London

Application hosted on Vercel in the London region

33

Granular permissions for custom roles

Contents

01 Security overview

Hosting, tenant isolation, audit trail, encryption and monitoring

02 Sub-processors and data recipients

Who processes data for QWTN, what they do and where

03 Information security policy

How QWTN runs security day to day

04 Access control

Roles, permissions, approvals, MFA, single sign-on and platform access

05 Incident response

How incidents are detected, handled and reported

06 Business continuity and recovery

Resilience, backups and recovery

07 Service levels

Uptime target, service credits and support response

08 Security questionnaire answers

Answers to the security and privacy questions buyers ask most

This pack describes how QWTN is built and run, as at 15 October 2026. If your review needs something it does not cover, email security@qwtm.co.uk.

Data Processing Agreement

The UK GDPR Article 28 agreement is not repeated in this pack. It is published on our website at <https://www.qwtm.co.uk/dpa>, and every legal document is at <https://www.qwtm.co.uk/legal>.

01

Security overview

How QWTN is built and run to protect your records. Version 1.0, 15 October 2026.

Ireland

Customer records stored on AWS, in the eu-west-1 region

London

Application hosted on Vercel in the London region

Every table

Row level security switched on across the production database

What QWTN is

QWTN is a multi-tenant web application for UK waste carriers. It covers waste transfer notes, hazardous consignment notes, collections and scheduling, fleet and driver compliance, health and safety records, quotes and invoices, a customer portal and a public API. It is operated by WhealBit, trading as QWTN, Penzance, Cornwall.

You are the controller of the personal data you record in QWTN. QWTN is your processor under UK GDPR. The Data Processing Agreement is published at <https://www.qwtm.co.uk/dpa>, and the full set of legal documents is at <https://www.qwtm.co.uk/legal>.

Where your data is held

Component	Provider	Location
Database, sign-in and file storage	Supabase (PostgreSQL 17)	AWS, Ireland (eu-west-1)
Application hosting	Vercel	London (region lhr1)
Static website assets	Vercel edge network	Global. No customer records are cached
Transactional email	Resend	United States
Bot protection on sign-up	Cloudflare Turnstile	Global
Rate-limit counters	Upstash	No customer records held
Product analytics	PostHog EU cloud, only after you accept analytics cookies	EU

All customer records are stored in Ireland. The application code that handles them runs in London. Email is the one route that leaves the UK and EU, because outbound messages pass through Resend in the United States. The full list of suppliers is in the sub-processors document.

Keeping each customer's data apart

Every QWTN customer is a team, and the database itself enforces the boundary between teams.

- Row level security is switched on for every table in the production database. It was checked against the live project on 15 October 2026. Each query is limited to the signed-in user's team, and the check runs inside the database, so it holds whatever the application layer does.
- Restrictive rules sit on top of the team rules. Read-only auditors cannot add, change or delete anything. Members limited to a depot cannot see records from other depots.
- Administrative and internal data cannot be read from the browser or with a public API key at all. Only QWTN's server-side code can reach it.
- Where server-side code does act on a team's data, it works out the team from the signed-in user's membership, never from a value sent in the request.
- The isolation rules were load-tested at scale, and the automated test suite covers permissions, roles and the API gate.

A tamper-resistant audit trail

QWTN keeps an append-only change history for the records that matter: waste transfer notes, consignment notes, collections, clients and contacts, sites, containers, invoices, payments, credit notes, quotes, contracts, price lists, vehicles and maintenance, team members, roles and team settings.

- Every insert, update and delete is recorded by the database. Application code cannot skip it.
- Each event stores who made the change (user and role), when, where it came from (the app, the driver app, the API, the system or a scheduled job), the action, a field-by-field before and after and, for deletions, a snapshot of the record. Fields holding passwords, secrets, tokens and key hashes are never written to the trail. Changes made with an API key are attributed to that key.
- Entries cannot be edited or deleted by customer users or by application code. They are removed only by the per-team retention process once the retention period ends.
- Each team sets its own retention. The default is 7 years and the minimum is 3 years. A legal hold on clients, notes, consignment notes, invoices and collections stops both deletion of the record and purging of its history.
- Owners, admins and auditors can read their team's events and export them.
- Sign-ins and multi-factor authentication events are logged with IP address and device, and every action taken by QWTN platform administrators is logged separately.

7 years

Default audit trail retention. Each team can change it, with a 3 year minimum

Append-only

Customer users and application code cannot edit or delete audit entries

Access control

The access control document has the detail. In short:

- Six built-in roles (owner, admin, office, finance, driver, auditor) and custom roles built from a catalogue of 33 granular permissions.
- Approval rules for credit notes, write-offs, client deletion, note deletion, pricing changes and billing runs, with optional value thresholds. An approved request runs through the same checks as the original, so validation is not bypassed.
- A read-only auditor role enforced in the database and at the API.
- Authenticator-app multi-factor authentication with ten one-time recovery codes, a team policy that can require it by role, a team idle-session timeout from 15 minutes to 8 hours and an option to enforce single sign-on.
- SAML single sign-on and SCIM 2.0 provisioning for teams that use them.
- Access for QWTN platform administrators is restricted to authorised team members, and every administrative action is logged.

Health and safety photos are private

They are held in private storage, scoped to the team that owns them and opened with short-lived signed links. In place since 15 October 2026.

Encryption and credential handling

- **In transit.** All traffic uses HTTPS. HSTS is sent with a one-year lifetime, covers subdomains and is preloaded.
- **At rest.** Supabase encrypts the database and file storage with AES-256 and Vercel encrypts its infrastructure, under each provider's published terms.
- **Secrets encrypted by QWTN as well.** Payment provider keys, telematics credentials, OAuth tokens and webhook signing secrets are encrypted with AES-256-GCM under a dedicated key. DEFRA Digital Waste Tracking credentials are encrypted with AES-256-GCM under a separate key.
- **Hashed credentials.** Customer portal PINs are hashed with scrypt and a random salt per PIN. API keys, SCIM tokens and multi-factor recovery codes are stored only as SHA-256 hashes. API keys are shown once, when they are created.
- **Passwords.** Passwords are handled by the sign-in service, not by QWTN code. Leaked-password protection is on: passwords found in the HaveIBeenPwned breach corpus are rejected.
- **Card data.** Card details never reach QWTN servers. Checkout uses Stripe's hosted and embedded payment elements.
- **Private photo storage.** Health and safety photos, which can show people and vehicle registrations, are held in private storage. Access is scoped to the team that owns them and uses short-lived signed links. This has been the case since 15 October 2026. Job photos are private in the same way.

Application security

- Every page carries a Content-Security-Policy that names the origins it may load from, plus protection against clickjacking and content-type sniffing, a strict referrer policy and a permissions policy that limits camera, microphone and location access.
- Rate limiting protects the public API, sign-in routes, signing and share links, public forms and exports. Public API keys are limited to 120 requests a minute each.
- Public API keys carry named scopes (16 scopes, or full access), can expire, can be revoked at any time and support idempotency keys for safe retries.
- Outbound webhooks are signed with HMAC-SHA256 over a timestamp and the body, so receivers can reject forged or replayed calls. Signing secrets can be rotated without downtime. QWTN refuses to deliver webhooks to private, loopback or link-local addresses. Failed deliveries are retried on a schedule over about three days.
- Share and signing links use signed, unguessable tokens that can be revoked. Signing links expire after 7 days by default.
- Scheduled-job endpoints reject any request that does not carry the correct secret.
- Cloudflare Turnstile protects sign-up from automated abuse.
- Testing environments cannot send email to real customers or use live payment keys.

Monitoring and alerting

- Unhandled errors from every route, page and server action are captured with the route they came from.
- Slow and failed API requests are recorded and kept for 30 days.
- Every scheduled job run is logged with its status and duration. A failed run emails the QWTN team straight away.
- The QWTN team is alerted by email to error spikes, failed scheduled jobs, a backed-up job queue and stuck or repeatedly failing jobs. Alerts are de-duplicated across servers so a long incident produces a manageable stream.
- A public health check covers the database, sign-in, file storage, background jobs, and email and payment configuration. It reports a failure when core services are down, so external monitors can poll it. A public status page at <https://www.qwtm.co.uk/status> shows the live state.
- Operations, performance and audit views bring these records together for the QWTN team.

Data retention and deletion

Data	Retention
Customer records	The life of the account. After closure, kept for 30 days (the account can be reopened and data exported in that time), then deleted automatically
Audit events	Set per team: default 7 years, minimum 3 years

Data	Retention
Demo workspaces	Deleted after they expire
Background job result files	14 days
Background job records	90 days
API timing samples	30 days
Webhook event records	30 days
API idempotency keys	24 hours

Users can download their team's records from the app at any time, which supports data subject access and portability requests under UK GDPR Articles 15 and 20. The download is limited by row level security to the user's own team.

Resilience

- Scheduled jobs run every day, covering Environment Agency re-verification, collection generation, reminders and platform housekeeping.
- The background job queue is crash-safe. It claims work so that two workers never take the same job, saves a checkpoint after every slice, hands back a job whose worker has stopped and refuses writes from a worker that has lost its claim.
- Database changes are additive. For larger changes a rollback script is prepared before the change is applied.
- Supabase takes automated database backups, and a restore from backup has been tested.
- Vercel keeps previous production deployments, so the last good release can be re-promoted if a release goes wrong.

Responsible disclosure

If you find a vulnerability, email security@qwtm.co.uk. The disclosure policy is published at <https://www.qwtm.co.uk/security>.

Related documents

Sub-processors, information security policy, access control, incident response, business continuity, service levels and security questionnaire answers are in this pack. Public legal pages: <https://www.qwtm.co.uk/dpa>, /sub-processors, /sla, /privacy, /terms, /security and /status.

02

Sub-processors and data recipients

The suppliers that help QWTN deliver the service, what they do and where. Version 1.0, 15 October 2026. The live list is published at <https://www.qwtm.co.uk/sub-processors> and forms an annex to the Data Processing Agreement at <https://www.qwtm.co.uk/dpa>.

Customer records are stored in Ireland

The application runs in London. Email is the one route that leaves the UK and EU, because outbound messages pass through Resend in the United States.

Sub-processors

These suppliers process customer personal data on QWTN's behalf.

Sub-processor	What it does for QWTN	Customer data involved	Location
Supabase, Inc.	Application database (PostgreSQL 17), user authentication including authenticator-app MFA and SAML single sign-on, and file storage for photos, logos, generated exports and producer documents	All records in the service: team members, clients and contacts, waste transfer notes and signatures, consignment notes, collections, fleet, driver and health and safety records (including accident book entries), quotes, invoices, portal access records and the audit trail	AWS, Ireland (EU)
Vercel, Inc.	Hosts the application, runs serverless functions and scheduled jobs, keeps request and function logs	Data in requests and responses while the service runs. IP address and device details in logs	Functions in London. Static assets are served from a global edge network that carries no customer records. Vercel states that some support and logging processing takes place in the United States

Sub-processor	What it does for QWTN	Customer data involved	Location
Resend, Inc.	Sends every email the service sends: shared notes, signature requests, invitations, quotes, invoices and reminders, driver schedules, accident and injury-reporting alerts, portal login codes and operational alerts	Recipient name and address, subject and body (which can include a link and summary details of the record), delivery and open status	United States
Cloudflare, Inc. (Turnstile)	Bot protection on sign-up	IP address, browser signals and a challenge token. No records	Global
Upstash, Inc.	Rate-limit counters	A counter keyed by IP address or account identifier that expires within minutes. No record content	No customer records held
PostHog, Inc. (EU cloud)	Product analytics, loaded only after the user accepts analytics cookies	A pseudonymous identifier, IP address, device, pages and events. Record content is never sent	EU
Heidelberg Institute for Geoinformation Technology (OpenRouteService)	Road distances and route geometry for the route planner, used only when a team switches on route optimisation	Latitude and longitude of the day's stops, depot and tip sites, as coordinate pairs. No names, addresses or references are sent	Provider based in Germany (EU)

Services that act for you, using your own account

QWTN connects to these with credentials you supply, and your contract with the provider governs the data they hold. Credentials are stored encrypted.

Service	Use	Data sent by QWTN
Stripe (your own account)	Invoice payment links	Invoice number, amount in pence, and QWTN invoice and team identifiers as metadata
GoCardless (your own account)	Direct Debit payment requests	Invoice number, amount and QWTN invoice identifier
Webfleet, Samsara, Microlise (your own account)	Reading vehicle positions and details	Nothing about individuals. QWTN reads from the provider
DEFRA Digital Waste Tracking (UK Government)	Submitting waste movement receipts when you switch it on and instruct it	The receipt data you choose to submit, authenticated with your DWT credentials
Webhook endpoints you configure	Event delivery	The event payload, signed with HMAC-SHA256

Independent controllers and public data sources

These are not sub-processors.

Service	Purpose	Data involved	Status
Stripe Payments UK Ltd / Stripe, Inc.	Billing for QWTN subscriptions	Account holder name, email, billing details and card data entered at Stripe	Independent controller. Card numbers never reach QWTN
Companies House	Company lookup	The company name or number the user searches for	Public data source
Environment Agency public registers	Carrier, permit and exemption lookups and daily re-verification	Registration numbers, names or postcodes	Public data source
postcodes.io	Postcode to location	The postcode	Public data source
Clearbit autocomplete	Suggests a company website and logo during set-up	The company name typed	Third-party data source
Google Fonts	Fonts in the app	Visitor IP address and browser data	Independent controller for its request logs
OpenStreetMap tile servers and Esri imagery	Map tiles	Visitor IP address and the map area	Independent controllers for their request logs

Changes to this list

QWTN updates the published list and gives customers at least 30 days' notice by email to the account owner before a new or replacement sub-processor starts processing customer personal data. A customer may object on reasonable data protection grounds within that period, as the Data Processing Agreement provides. Urgent replacements needed to keep the service running are notified as soon as reasonably practicable.

Transfers outside the UK

Customer records are stored in Ireland, which the UK treats as adequate. Processing by Resend, Cloudflare and Vercel's United States support and logging teams is a restricted transfer. QWTN relies on the UK-US Data Bridge where the supplier is certified under it, and otherwise on the supplier's standard contractual clauses with the ICO's UK Addendum, as set out in each supplier's data processing terms.

03

Information security policy

How QWTN runs information security. Version 1.0, 15 October 2026. It describes controls that exist in the system today.

Report a vulnerability

Email security@qwtm.co.uk. The disclosure policy is at <https://www.qwtm.co.uk/security>.

Scope and responsibility

The QWTN team is accountable for security, privacy and operations. Production access is limited to authorised team members. The policy covers the QWTN application, its database and storage, its deployments, its third-party services and the data of its customers.

Contacts:

- security@qwtm.co.uk for vulnerability reports. The disclosure policy is at <https://www.qwtm.co.uk/security>.
- privacy@qwtm.co.uk for data protection.
- hello@qwtm.co.uk for support.

How customer data is separated

Every customer is a team. Row level security on every table limits each query to the signed-in user's team, with restrictive rules for the read-only auditor role and for depot-limited members. Internal tables are reachable only by QWTN's server-side code. The security overview and access control documents give the detail.

How access is granted and removed

Roles, granular permissions, approvals, MFA policy, idle timeout, single sign-on and SCIM provisioning are described in the access control document. Removing, suspending or deprovisioning a user revokes all of their sessions. QWTN platform administrator access is limited to authorised team members, and every action is logged.

How secrets and keys are handled

- Secrets are held as protected configuration in the hosting platform. Only values deliberately marked public reach the browser. The database's privileged service key is used server-side only.

-
- The application refuses to start if its core database configuration is missing.
 - Customer-supplied provider credentials and webhook signing secrets are encrypted with AES-256-GCM under a dedicated key. DEFRA Digital Waste Tracking credentials are encrypted under a separate key.
 - API keys, SCIM tokens and multi-factor recovery codes are stored as hashes. Portal PINs are stored with script and a salt.
-

How changes are made

- Code is held in version control. Every branch is built as a preview deployment before it is merged, and the main branch is built for production.
 - An automated test suite of more than 1,200 tests, all passing on 15 October 2026, covers permissions, the audit trail, billing, the API gate, webhooks, portal access, the job queue, monitoring, the email and payment safety guard. The whole codebase is also checked by a strict type checker.
 - Database changes are numbered, version-controlled scripts. They are additive, most are safe to re-run, and larger ones have a rollback script prepared before they are applied.
 - Non-production deployments cannot email customers outside an allowlist or use a live payment key.
-

How data is protected in transit and at rest

HTTPS everywhere, with HSTS (one year, subdomains, preload). The database and file storage are encrypted at rest by Supabase. Secrets are encrypted again by the application, as above. Responses carry a Content-Security-Policy limited to named origins, clickjacking protection and content-type sniffing protection.

How activity is recorded and watched

- An append-only audit trail with attribution covers the core business records. Retention is set per team (default 7 years, minimum 3), with legal hold.
- Sign-in events, administrator actions, scheduled job runs, unhandled errors and sampled API timings are stored and reviewable by the QWTN team.
- The QWTN team is alerted by email to error spikes, failed scheduled jobs, a backed-up job queue and failing or stuck jobs.
- A public health check and a status page at <https://www.qwtm.co.uk/status> show the live state of the service.

The security overview gives the detail.

How data is kept and deleted

Customer records are kept for the life of the account. Audit events follow each team's retention setting. Demo workspaces are deleted on expiry. Job files are kept for 14 days, job records for 90 days, timing samples for 30 days, webhook events for 30 days and idempotency keys for 24 hours. When an account is closed, its records are kept for 30 days so the team can export them or reopen the account, then deleted automatically. Users can export their records from the app at any time.

How third parties are managed

Each sub-processor is engaged on its standard written data processing terms. The list, locations and purposes are in the sub-processors document and at <https://www.qwtn.co.uk/sub-processors>. Customers get at least 30 days' notice of a new sub-processor and may object.

How vulnerabilities are handled

Reports go to security@qwtn.co.uk. Dependencies are version-locked, so every build uses exactly the packages that were tested.

How incidents and outages are handled

See the incident response and business continuity documents.

Acceptable use of the service

Customers agree to the acceptable use policy at <https://www.qwtn.co.uk/acceptable-use>. Rate limits and bot protection apply to public routes.

04

Access control

How access to QWTN is controlled, for your users inside the product and for QWTN platform administrators. Version 1.0, 15 October 2026.

6

Built-in roles

33

Granular permissions for custom roles

Read-only

Auditor role enforced in the database and at the API

Roles and permissions for your users

Built-in roles

Role	Purpose	Permissions
Owner	Full access, including plan and billing. Cannot be removed	All 33 permissions
Admin	Everything except plan and billing	32 of 33 (all but billing management)
Office	Day-to-day operations: clients, jobs, notes, invoices, fleet and compliance	View everything, plus manage notes, collections, clients, containers, fleet, compliance, finance and portal access
Finance	Quotes, invoices, credit notes, reports and exports	View notes, collections, clients, finance and reports. Manage finance and portal access. Export data
Driver	The driver app: assigned jobs, transfer notes and walkaround checks	View and create notes, view and complete assigned collections, view fleet
Auditor (read-only)	Compliance reviews	View records and reports, and view the audit log

Drivers see their own notes and the notes on jobs assigned to them. Office-type roles read all team data, and editors change it.

Custom roles

Teams build their own roles from a catalogue of 33 permissions in four groups:

- **Operations:** notes, collections, clients and containers.
- **Fleet and compliance.**
- **Finance:** credit notes, payments, pricing and billing runs are separate permissions.

-
- **Administration:** reports, data export, audit view, team management, role management, depots, security settings, API and integrations, legal hold, approvals, settings and billing.

When permissions were split into finer ones, existing roles kept access they already had, so no team lost a capability. Role changes are recorded in the audit trail.

Enforcement at three layers

- **Database.** Row level security scopes data to the team. Restrictive rules make auditors read-only whatever the application does, and hide records from members limited to certain depots.
- **API gate.** Every non-public API request is checked for the multi-factor level your team policy requires. Writes from auditors are rejected, apart from their own account settings, sign-in, notifications and favourites.
- **Routes.** Each route checks the specific permission it needs before it acts.

Approvals

Each team can set approval rules per action: credit notes, write-offs, client deletion, note deletion, pricing changes and billing runs, each optionally with a value threshold. A matching request is held until someone with approval permission approves or rejects it. An approval replays the original request through the same checks, so validation and side effects are unchanged. Requests are visible to office roles and to the person who made them.

Authentication

- Passwords and sessions are handled by the sign-in service. QWTN code never sees or stores passwords. Leaked-password protection is on, so passwords from known breaches are rejected.
- Authenticator-app (TOTP) multi-factor authentication. A user with a verified factor must complete the challenge before using the app, and a user whose team policy requires MFA must enrol first.
- Ten one-time recovery codes per user, shown once and stored only as hashes.
- A team security policy sets which roles must use MFA, an idle-session timeout of 15, 30, 60, 120, 240 or 480 minutes, and an option to enforce single sign-on.
- SAML single sign-on, set up per team with its own domains.
- SCIM 2.0 user provisioning with a per-team token that is shown once and stored as a hash. Deprovisioning a user through SCIM revokes their sessions.
- Login history (sign-ins and MFA events, with IP address and device) is available to users with audit permission.

Joiners, movers and leavers

- **Joining.** An owner, or a user with team management permission, invites people by email. The invitation is a single-use link with an expiry, and only a hash of the token is stored.
- **Moving.** A change to a member's role or depot scope takes effect on their next request and is recorded in the audit trail.
- **Leaving.** Removing a member, suspending them, deprovisioning them through SCIM or resetting their MFA each revokes every session they hold. Membership is checked on each request, so access ends sooner than

token expiry would.

API and integration access

- API keys are shown once and stored only as a hash and a short prefix. You choose from 16 scopes (notes, clients, sites, collections, containers, invoices, quotes, consignments, weighbridge and audit, read or write as applicable) or full access. Keys can carry an expiry of up to two years, can be revoked at any time and record their last use and IP address. The default limit is 120 requests a minute per key. Activity through a key is attributed to the key in the audit trail.
 - Webhook endpoints are managed by users with API permission. Signing secrets are encrypted at rest and can be rotated without downtime.
 - Provider credentials you supply for payments, telematics and DEFRA Digital Waste Tracking are encrypted with AES-256-GCM.
-

Customer portal access

The portal is for your own clients. Contacts get access by invitation from a user with portal permission. They sign in with a PIN (hashed with scrypt) or a login code, can use multi-factor authentication, and see only the records scoped to their own client. Access links expire and can be revoked.

QWTN platform administrator access

- Platform administration is limited to authorised members of the QWTN team. Only the platform owner can add or remove administrators.
 - Administration can be set to require an authenticator-app session.
 - Every administrative action is logged with who did it, what it was, what it affected, the detail and the IP address.
 - Production data is reachable only through the database and hosting accounts, which only authorised team members can open. The privileged database key is a server-side secret and is never sent to the browser.
 - Administrative data is not reachable by customer sessions or API keys.
 - Support actions that act on a customer's data, such as erasing a team, are explicit, logged operations.
-

Reviewing access

- Team owners can see who has access, their roles and the login history, and can export the audit trail.
 - Owners set the audit trail retention and can place legal holds.
-

05

Incident response

How QWTN detects, handles and reports security and operational incidents. Version 1.0, 15 October 2026. The QWTN team carries out every role described here.

48 hours

Where practicable, QWTN notifies a customer of a personal data breach affecting their data within 48 hours of becoming aware, and without undue delay in every case.

How incidents are detected

Signal	What it catches	Where it goes
Error capture on every route, page and server action	Application failures	The QWTN operations views
Error-spike alert	A sudden fault	Email to the QWTN team
Failed scheduled job alert, sent as soon as a run fails	Failed daily jobs, such as collection generation, reminders, Environment Agency re-verification and DEFRA submissions	Email, and the operations views
Background job alerts	A backlog, stuck jobs or repeated failures, meaning background work is not running	Email, and the operations views
Slow and failed request timings, kept for 30 days	Performance and error trends by route	The performance views
Public health check and status page	Database, sign-in, storage, job queue, email and payment configuration	Public. Reports a failure when core services are down
Sign-in history, administrator action log and the audit trail	Unusual sign-ins, administrator actions and data changes	The audit views. Team owners see their own team's events
Reports to security@qwtm.co.uk or hello@qwtm.co.uk	Anything a customer or researcher notices	The QWTN team mailbox

Alerts are de-duplicated across servers, so a long incident produces a manageable stream of emails rather than a flood. Failed scheduled jobs are alerted at once.

What happens when an incident is found

- 1. Confirm and scope.** The team checks the operations views (errors, scheduled jobs, background jobs), the health check and the hosting platform's function logs. For a suspected data issue, the audit trail for the team and period shows who (user, role or API key), when, the source and the field-level change. The sign-in history shows sign-ins with IP address and device, and the administrator action log shows every platform action.
 - 2. Contain.** The team can:
 - end a user's access by removing or suspending the member, resetting their MFA or deprovisioning them through SCIM, each of which revokes all of their sessions;
 - revoke an API key, rotate a webhook signing secret or disable the endpoint;
 - rotate secrets and encryption keys in the hosting and database platforms and redeploy;
 - revoke share links (signing links also expire after 7 days);
 - require an authenticator-app session for platform administration;
 - re-promote the previous production deployment.
 - 3. Recover.** The team fixes forward in version control and deploys. For a faulty database change, it applies the rollback script prepared before the change. For data loss, it restores from the database platform's automated backups. A restore from backup has been tested.
 - 4. Preserve evidence.** The audit trail is append-only, so application code cannot alter it. The hosting and database providers keep their own logs under their retention terms.
 - 5. Notify.** See the next section.
 - 6. Review.** The team records what happened and what changed. Fixes are made in code and database scripts, so they are version-controlled and, where practical, covered by tests.
-

Notifying customers and regulators

- **Personal data breach affecting customer personal data.** QWTN notifies the customer's named contact, or the account owner, without undue delay and, where practicable, within 48 hours of becoming aware, as the Data Processing Agreement provides. The notice states what happened, the data and people affected as far as known, the likely consequences and the measures taken. Notices are sent by email and, where needed, directly.
 - **Your decisions as controller.** You decide whether to notify the ICO within 72 hours of becoming aware, and whether to notify data subjects.
 - **Data QWTN controls itself.** For account, billing and website data, QWTN assesses the breach and reports it to the ICO within 72 hours where the law requires it.
 - **Service incidents** are shown on the public status page at <https://www.qwtn.co.uk/status>.
-

Reporting a security issue to QWTN

Email security@qwtn.co.uk. The disclosure policy is published at <https://www.qwtn.co.uk/security>.

06

Business continuity and recovery

What keeps QWTN running and how it recovers. Version 1.0, 15 October 2026.

Backup restore tested

Supabase takes automated database backups, and a restore from backup has been tested.

Architecture that limits the impact of a failure

- **Managed platforms.** The application runs on Vercel in London, with no servers for QWTN to patch or restart. The database, sign-in and file storage run on Supabase in Ireland.
- **Stateless application.** All state lives in the database and storage, so a failed function invocation is simply retried by the next request.
- **Crash-safe background work.** The job queue claims work so that two workers never take the same job, saves a checkpoint after every slice, returns an expired claim to the queue and refuses writes from a worker that has lost its claim. A worker that stops part-way through a job neither loses nor repeats work. While someone is watching a job, a stalled job restarts its worker.
- **Safe retries.** Invoice reminders, incident and injury-reporting alerts and bulk sends use idempotency keys, so a retry never sends twice. API writes accept idempotency keys. Invoice reminders are idempotent per invoice, type and day. Collection generation is idempotent per schedule and date. Webhook deliveries retry on a schedule over about three days.
- **Graceful degradation.** Route planning falls back to a labelled straight-line estimate if the routing provider is unavailable. Subscription price lookup falls back to known prices. Email and payment status show as not configured rather than failing.
- **Continuity for your team.** Users can export their records as CSV and PDF, and as background ZIP exports. Work done in the driver app while offline is queued and replayed when the connection returns.

Backups and data recovery

- Supabase takes automated database backups, and a restore is carried out through Supabase. A restore from backup has been tested.
- The audit trail records changes to the core records with old and new values. This supports repairing individual records without restoring a whole database.

Recovering from a faulty release

- Vercel keeps previous production deployments, and the previous one can be re-promoted.
- Database changes are additive. For larger changes a rollback script is prepared before the change is applied and kept with it.

If a supplier has a problem

Supplier	Effect	What continues
Supabase	The app cannot load or save records, and sign-in fails	The status page shows it
Vercel	The app is unreachable	Your data is untouched in the database
Resend	Outgoing email fails	Each failure is reported to the user as "email did not go". Nothing is faked, and records are saved
Stripe	Subscription checkout and the billing portal fail	Existing access continues
OpenRouteService	Road distances are unavailable	Straight-line estimates, clearly labelled
DEFRA Digital Waste Tracking	Submissions fail and retry with back-off	Receipts are kept and retried

Operational alerting for these events is described in the incident response document.

People and resources

The QWTN team runs the service. Production access, the database and hosting accounts and the keys are limited to authorised team members. The managed platforms keep running without intervention.

07

Service levels

The service levels QWTN publishes, and how the service is hosted and monitored. Version 1.0, 15 October 2026. The full Service Level Agreement is at <https://www.qwtm.co.uk/sla>.

99.5%

Monthly uptime target

5% to 25%

Service credits on Eligible Plans

1 business day

Target initial response on the Fleet plan

Uptime target

For an Eligible Plan, we aim to keep the Service Available with a Monthly Uptime Percentage of at least 99.5% in each calendar month.

- An Eligible Plan is the Fleet plan, or any other plan or written order that expressly references the SLA. For the Free, Solo and Carrier plans the same figure is a non-binding target and no service credits are available.
- "Available" means the core application at [qwtm.co.uk](https://www.qwtm.co.uk) (signing in, creating, signing and viewing waste transfer notes, and the dashboard) is materially accessible, as measured by QWTN's monitoring systems.

Service credits for Eligible Plans, as a percentage of the monthly fee for the affected service:

Monthly uptime	Credit
Less than 99.5% but at least 99.0%	5%
Less than 99.0% but at least 98.0%	10%
Less than 98.0% but at least 95.0%	15%
Less than 95.0%	25%

Claims are made in writing to hello@qwtm.co.uk within 30 days after the end of the month. Exclusions, including scheduled maintenance and third-party infrastructure, are set out in the SLA. Credits are capped at 100% of the month's fee and sit inside the overall liability cap in the Terms.

Support response targets

These are targets for an initial response, measured in business hours (09:00 to 17:00 UK time, Monday to Friday, excluding bank holidays in England and Wales) from receipt of a complete request by email to hello@qwtn.co.uk.

Plan	Target initial response
Free	Best efforts
Solo	2 business days
Carrier	2 business days
Fleet (dedicated support)	1 business day

Maintenance

QWTN gives reasonable advance notice of scheduled maintenance, by in-app notice or email, and carries it out off-peak where practicable.

How the service is hosted and run

Item	Detail
Application	Next.js on Vercel, with functions in London
Data	Supabase PostgreSQL 17, sign-in and file storage, on AWS in Ireland
Scheduled work	Ten jobs run each day, including Environment Agency re-verification, collection generation, the background job worker, platform housekeeping and alert checks, and invoice and licence reminders
Backups	Automated database backups by Supabase. A restore has been tested
Health check	Public, with no customer data. Covers the database, sign-in, file storage, background jobs, and email and payment configuration, and reports operational, degraded or down
Status page	https://www.qwtn.co.uk/status , checked live on every load

Monitoring and alerting

- Unhandled error capture across all routes, pages and server actions, plus API timing records for slow requests, server errors and a sample of normal traffic, kept for 30 days. Every scheduled job run is logged with its status and duration.
- Email alerts to the QWTN team for an error spike, a failed scheduled job (immediately), a job queue backlog, stuck jobs and repeated job failures, de-duplicated so each issue produces a manageable number of emails.

08

Security questionnaire answers

Answers to the questions buyers most often ask, in the style of SIG Lite and CAIQ. Version 1.0, 15 October 2026. Each answer reflects how QWTN works today. If your questionnaire asks something that is not covered here, email security@qwtm.co.uk.

Data Processing Agreement

The UK GDPR Article 28 agreement is published at <https://www.qwtm.co.uk/dpa>.

1. Organisation and governance

#	Question	Answer
1.1	Legal entity	WhealBit, trading as QWTN, Penzance, Cornwall
1.2	Named security contact and disclosure route	Yes. security@qwtm.co.uk . A security.txt file is published and the disclosure policy is at https://www.qwtm.co.uk/security
1.3	Written information security policy	Yes. It is included in this pack
1.4	Who has production access	Limited to authorised members of the QWTN team
1.5	Published data protection contact	Yes. privacy@qwtm.co.uk

2. Data protection agreements and sub-processors

#	Question	Answer
2.1	UK GDPR Article 28 data processing agreement available	Yes. It is published at https://www.qwtm.co.uk/dpa
2.2	Published sub-processor list with change notice	Yes. https://www.qwtm.co.uk/sub-processors . Customers get 30 days' notice of a new sub-processor and a right to object

3. Hosting, location and data residency

#	Question	Answer
3.1	Where is customer data stored	In Ireland, on AWS (eu-west-1), through Supabase
3.2	Where do application servers run	Vercel, London
3.3	Is customer data stored outside the UK or EU	No customer records are stored outside the UK or EU. Outbound email passes through Resend in the United States, and Vercel states that some support and logging processing takes place in the United States
3.4	Does QWTN run its own data centres or hardware	No. QWTN runs entirely on managed platforms, so no customer data sits on QWTN premises or hardware
3.5	Physical security	Provided by the hosting providers (AWS through Supabase, and Vercel)
3.6	Multi-tenant or single-tenant	Multi-tenant, with isolation enforced by the database

4. Data separation and protection

#	Question	Answer
4.1	How is one customer's data separated from another's	Row level security is enabled on every table in the production database, checked against the live project on 15 October 2026. Policies scope every row to the user's team
4.2	Are internal tables protected from the browser and the public API key	Yes. Administrative and internal tables cannot be read from the browser or with a public API key. Only QWTN's server-side code can reach them
4.3	Is isolation tested	Yes. Permission matrix, API gate, audit trail and role tests run in the automated test suite, and the isolation rules were load-tested at scale
4.4	Can non-production deployments email customers or take real payments	No. Email is limited to an allowlist and live payment keys are refused outside production
4.5	Special category data	Accident book and near-miss records can hold health data. They sit behind the same row level security and role controls, and access is by permission
4.6	Data minimisation controls	Photo and GPS capture are optional, visibility is role-based and each team sets its own retention
4.7	Are health and safety photos protected	Yes. They are held in private storage, scoped to the owning team and accessed with short-lived signed links. This has applied since 15 October 2026

5. Identity and access management

#	Question	Answer
5.1	Role-based access control	Yes. Six built-in roles and custom roles built from 33 permissions
5.2	Least privilege and a read-only role	Yes. The auditor role is read-only, enforced in the database and at the API
5.3	Approval workflow for sensitive actions	Yes. Credit notes, write-offs, client and note deletion, pricing changes and billing runs
5.4	Multi-factor authentication	Yes. Authenticator-app MFA for all users, with a team policy that can require it by role
5.5	MFA recovery	Yes. Ten one-time recovery codes, stored hashed
5.6	Single sign-on	Yes. SAML 2.0, with an option to enforce SSO for the team
5.7	Automated user provisioning	Yes. SCIM 2.0. Deprovisioning revokes the user's sessions
5.8	Session timeout	Yes. A team can set an idle timeout from 15 minutes to 8 hours
5.9	Can a user's sessions be revoked immediately	Yes. On removal, suspension, SCIM deprovisioning and MFA reset
5.10	Password storage and policy	Passwords are handled by the sign-in service and never reach QWTN code. Leaked-password protection is on, so passwords found in known breaches are rejected
5.11	Login history available to customers	Yes. Sign-ins and MFA events with IP address and device
5.12	Platform staff access to customer data	Limited to authorised members of the QWTN team. Every administrative action is logged, and administration can be set to require an authenticator-app session
5.13	Customer portal authentication	A PIN (hashed with scrypt) or a login code, optional MFA, and access scoped to the client

6. Encryption and key management

#	Question	Answer
6.1	Encryption in transit	Yes. HTTPS only, with HSTS for one year including subdomains and preload
6.2	Encryption at rest	Yes. The database and file storage are encrypted by Supabase, and Vercel infrastructure is encrypted by Vercel
6.3	Application-level encryption	Yes for secrets: customer integration credentials, OAuth tokens and webhook secrets (AES-256-GCM), and DEFRA Digital Waste Tracking credentials (AES-256-GCM under a separate key)

#	Question	Answer
6.4	Hashing of credentials	API keys, SCIM tokens and recovery codes use SHA-256. Portal PINs use scrypt with a per-PIN salt
6.5	Where are keys stored	As protected configuration in the hosting platform, server-side only, with dedicated keys for integrations and for DEFRA Digital Waste Tracking

7. Application security and development

#	Question	Answer
7.1	Source control and deployment pipeline	Version control. Vercel builds a preview per branch and builds production from the main branch
7.2	Automated tests	Yes. More than 1,200 automated tests, all passing on 15 October 2026, plus a strict type check of the codebase
7.3	Database change control	Numbered, version-controlled scripts. Changes are additive, with a rollback script prepared before larger changes
7.4	Security headers	Content-Security-Policy, clickjacking protection, content-type sniffing protection, referrer policy, permissions policy and HSTS
7.5	Input validation and injection protection	Queries are parameterised through the database client, filter input is sanitised and request bodies are validated on the server
7.6	Rate limiting and abuse protection	Yes. Applied to sign-in routes, signing links, public forms, exports and the API (120 requests a minute per key by default). Cloudflare Turnstile protects sign-up
7.7	SSRF protection for outbound webhooks	Yes. Delivery refuses private, loopback and link-local addresses
7.8	Public API security	Scoped keys (16 scopes), hashed at rest, optional expiry, revocable, idempotent writes and audit attribution
7.9	Webhook authenticity	HMAC-SHA256 over a timestamp and the body, with a short replay window and secret rotation

8. Logging and monitoring

#	Question	Answer
8.1	Are changes to customer records logged	Yes. An append-only audit trail with user, role, time, source, action and field-level change
8.2	Is the audit trail tamper-resistant	Yes. Customer users and application code cannot edit or delete entries. They are removed only by the per-team retention process once the retention period ends

#	Question	Answer
8.3	Customer access to audit data	Yes. Owners, admins and auditors can view and export their team's events
8.4	Audit retention	Set per team. Default 7 years, minimum 3 years. Legal hold prevents purging
8.5	Administrator action logging	Yes. Every platform administrator action is logged with actor, target, detail and IP address
8.6	Application error monitoring	Yes. All unhandled errors from routes, pages and server actions are captured
8.7	Alerting	Yes. Email alerts for error spikes, failed scheduled jobs, job backlog, and stuck or failing jobs
8.8	Health check and status page	Yes. A public health check and a status page at https://www.qwtm.co.uk/status
8.9	Log retention	API timing samples 30 days, job records 90 days, webhook events 30 days. Provider logs follow Vercel and Supabase retention

9. Incident management

#	Question	Answer
9.1	Documented incident response process	Yes. It is included in this pack
9.2	Customer breach notification time	Without undue delay and, where practicable, within 48 hours of becoming aware, as the Data Processing Agreement provides
9.3	Ability to contain a compromised account or key	Yes. Session revocation, API key revocation, webhook secret rotation, secret rotation with redeploy, and rollback to the previous deployment

10. Business continuity and backups

#	Question	Answer
10.1	Backups	Yes. Supabase takes automated database backups
10.2	Has a restore been tested	Yes. A restore from backup has been tested
10.3	Infrastructure resilience	QWTN runs on managed platforms operated by Supabase and Vercel, with no servers for QWTN to patch or restart
10.4	Rollback of a faulty release	Yes. The previous Vercel deployment can be re-promoted, and the database rollback script applied
10.5	Crash-safe background processing	Yes. The job queue is checkpointed and lock-safe

#	Question	Answer
10.6	Customer data export	Yes. Self-service export as CSV, PDF and ZIP, and through the API
10.7	Published uptime target	99.5% monthly. Credit-backed on the Fleet plan and non-binding on other plans

11. Privacy

#	Question	Answer
11.1	Role under UK GDPR	Processor for customer records. Controller for account, billing and website data
11.2	Data subject request support	Yes. Search, edit, export, change history, legal hold and erasure of a team
11.3	Deletion on termination	Yes. A 30-day export grace period, then deletion of the team's records. Backups age out
11.4	Sub-processors	Supabase, Vercel, Resend, Cloudflare, Upstash, PostHog and OpenRouteService
11.5	International transfers	Customer data stays in Ireland. Transfers to the United States rely on the UK-US Data Bridge or standard contractual clauses with the UK Addendum
11.6	Analytics and cookies	One non-essential technology, PostHog analytics, loaded only after consent
11.7	Is customer data used to train AI models	No. QWTN does not send customer data to any AI model provider

12. Personnel and third parties

#	Question	Answer
12.1	Confidentiality undertakings	Yes. The Data Processing Agreement binds QWTN to confidentiality
12.2	Supplier contracts	Each sub-processor is engaged on its standard written data processing terms
12.3	Customer integrations	Run with your own accounts and credentials, which are stored encrypted



Questions about security

Security reports

security@qwtm.co.uk

Privacy and data protection

privacy@qwtm.co.uk

Support

hello@qwtm.co.uk

Website

<https://www.qwtm.co.uk>

Data Processing Agreement

<https://www.qwtm.co.uk/dpa>

Live service status

<https://www.qwtm.co.uk/status>
