Tyten Technologies Limited

Company Number 16101444

25 Eccleston Place, London, England, SW1W 9NF

Effective Date: 18 November 2026

Version: 2.3

Previous Version: 2.2 (17 November 2026)

Tyten AI Privacy Policy

1. Who We Are

This Privacy Policy applies to the services provided by Tyten Technologies Limited ("Tyten", "we", "us", "our"), a company registered in England and Wales (Company No. 16101444), with its registered office at 25 Eccleston Place, London, England, SW1W 9NF.

We provide an AI-powered facilities management platform, including an AI helpdesk assistant, technician tools, an admin dashboard, mobile applications and backend integrations used by facilities management providers and their authorised end-users.

We are registered with the UK Information Commissioner's Office (registration number ZC021425). For the data our clients put into the Tyten platform, including details of their staff, suppliers and residents, we act as a processor on our clients' instructions, and the client is the controller.

For any questions about this Privacy Policy or our processing of personal data, please contact us at privacy@tyten.ai.

2. Scope

This Privacy Policy applies to all users of the Tyten AI solution, including:

- Residents interacting via WhatsApp, mobile apps, or similar interfaces
- Technicians using the Tyten mobile apps and tools
- Facilities managers and admin staff using the dashboard
- FM providers as enterprise clients
- Tyten's internal users supporting or maintaining the platform

3. Data We Collect

We collect and process the following types of information:

Category	Examples
Personal identifiers	Names, phone numbers, emails
Repair request content	Issue descriptions, error codes
Photo/video uploads	Media submitted to describe or verify faults
Work order data	Equipment ID, fix steps, diagnostic results
Device/session metadata	Device type, IP address, WhatsApp metadata
Diagnostic usage data	Timestamps, prompt usage, button clicks
Building and asset data	Equipment lists, floor plans, asset metadata
Location data	GPS data or address info (e.g. for technicians)
Voice data	WhatsApp voice messages or transcripts

3.1 Data Collected via the Tyten Mobile Apps

When you use the Tyten mobile applications distributed on the Apple App Store and Google Play Store, we additionally collect:

- Authentication tokens stored on-device in the iOS Keychain or Android Keystore. These do not leave the device except as the Authorization: Bearer header on requests to our API.
- Photos and videos taken with your device's camera or chosen from your photo library when you attach them to a work order. Videos, with sound, can be recorded only if your employer has turned this on, and the microphone is used only while you record a video. We request camera, microphone and photo-library permission only at the moment you tap the relevant control; the app does not access these continuously. Videos are kept with the rest of the job's data and are not sent to any AI provider. If you speak to fill in a form, your device's keyboard dictation turns your words into text, and the app receives only the text.
- Messages you send us from the app, such as a support message or a report of an AI answer you consider wrong, unsafe or offensive. A report includes the work-order reference and the answer you reported. Messages reach our support team by email, with your name and email address so that we can reply, and become support tickets. No AI service reads them. They are kept for as long as we need them to answer you and to check the AI guidance.
- Device identifiers (a non-resettable device model and operating-system version string) for crash diagnostics and to render the correct UI. We do not collect IDFA, AAID, or any cross-app advertising identifier.
- Push-notification tokens issued by Apple Push Notification service or Firebase Cloud Messaging, used solely to deliver work-order updates to your device.
- Precise location, during working time. Working time starts when the user marks themselves as on their way to, or arrived at, their first job of the day. It ends when their last job of the day is completed or marked as no access. If a job is left open, recording stops automatically after 14 hours, at midnight, or when the user signs out, whichever comes first. During working time the Tyten Jobs app records the device's location at intervals, more often when the user is moving. On iPhone, if the user allows it, this continues when the app is not on screen; on Android, only while the app is open. Before the device first asks for location permission, the app explains this and the user can decline. Location is used to record arrival and time on site on job sheets, including when the user forgets to mark a job as started, and to plan travel between jobs. It is not recorded outside working time and is not used for advertising.

4. How We Use This Data

We process the above data to:

- Route and resolve maintenance issues using AI tools
- Assist technicians with diagnostics and task documentation
- Generate work orders and update CAFM systems
- Deliver and monitor service quality for client companies
- Improve system performance and user experience
- Provide support and respond to client inquiries

5. Legal Bases for Processing

We rely on the following legal grounds under UK GDPR and related laws:

- Contract performance – For processing necessary to deliver our services to clients
- Legitimate interests – For platform monitoring, improvement, and internal reporting
- Legal obligation – For keeping financial records and meeting other legal and regulatory requirements
- Consent – For opt-in actions, such as WhatsApp messaging permissions

6. Sharing and Sub-Processing

We use selected service providers (sub-processors) to deliver the Tyten AI solution. The current sub-processors and the specific data shared with each are as follows:

Provider	Purpose
OpenAI, Anthropic, Google (Gemini)	AI processing within our automated workflows. For technician guidance we send the work-order title, description and any attached photo, and the provider returns suggested tools and diagnostic steps; no user account identifier is sent. For document and email processing (for example classification and data extraction) we send the content, which can include names and contact details. Data is processed under the provider's API terms (no model training on submitted content).
Meta (WhatsApp), Twilio	Communication interface for residents: phone numbers, message content, and delivery metadata used to send and receive WhatsApp/SMS messages.

AWS, GCP, Microsoft Azure	Hosting, storage, and server infrastructure for the platform and Customer Data.
Microsoft	Email processing through Microsoft 365 (Exchange and the Graph API): email content and sender and recipient addresses. Also internal operations and productivity tooling (email, document storage) used to support the Services.
Google (Workspace)	Tyten's own email and productivity tooling: email content and sender and recipient addresses, including messages users send us from the mobile apps.
Atlassian (Trello)	Support tickets: messages sent to our support mailbox, including messages users send us from the mobile apps, which can include names and contact details.
Xero	Accounting integration on a client's instruction: financial records and supplier data. Also Tyten's own invoicing: our clients' billing contacts and invoices.
Folk CRM	Customer relationship management: contact details of client representatives and prospective clients.

These sub-processors are approved by default and do not require individual client approval. A full and up-to-date list is available on request from privacy@tyten.ai.

7. Retention of Data

We retain data only for as long as necessary to:

- Fulfil our service obligations under client contracts
- Meet legal and regulatory requirements
- Comply with internal data retention schedules

7.1 Requests from Individual Users

Accounts for staff of our client companies are created and closed by the client company under its licence; users cannot close their own account. Such users can exercise their data protection rights, including deletion, by contacting the client company they work for. If they contact us at privacy@tyten.ai, we will pass the request to that client company without undue delay and help it respond.

Other individuals, such as residents, can make requests as set out in section 9.

7.2 Client Company Deletion and Export Requests

Client companies (enterprise customers) may additionally request export or deletion of all data associated with their tenant under their service agreement.

8. Data Security

We implement appropriate technical and organisational measures to protect personal data, including:

- Encryption in transit (TLS 1.2 or later) for web traffic, API calls and email, and encryption at rest for our servers' disks, document storage and database backup files
- Role-based access controls and least-privilege access
- Multi-factor authentication for administrative access
- Logging and monitoring of system access and security events
- Vulnerability management, patching, and secure development practices
- Incident response procedures and breach escalation
- Secure infrastructure provided by AWS, GCP, and Microsoft Azure
- Staff confidentiality undertakings and security awareness training

9. Your Rights

If your personal data is processed by Tyten, you may have the right to:

- Access your data
- Request correction or deletion
- Object to certain processing
- Request data portability
- Restrict processing in certain circumstances
- Withdraw consent at any time, where processing is based on consent
- Lodge a complaint with the UK Information Commissioner's Office (ICO) if you believe your data has been mishandled. The ICO's contact details are at https://ico.org.uk/make-a-complaint/. You may also complain to the supervisory authority of the EU member state where you live.

To exercise your rights, contact us at privacy@tyten.ai.

10. Updates to This Policy

This Privacy Policy may be updated to reflect legal, operational, or functional changes. Clients and affected users will be notified of material updates where applicable. The effective date and version number at the top of this document indicate when the latest version took effect.

11. Children's Data

The Tyten platform and mobile applications are intended for use by professional facilities-management staff and their authorised end-users, all of whom are adults in the course of their employment or residency. We do not knowingly collect personal data from children under 16. If we discover that we have inadvertently collected data from a person under 16, we will delete it within 30 days. Parents or guardians who believe a child has provided personal data should contact privacy@tyten.ai.

12. International Data Transfers

The Tyten platform and its data are hosted by AWS in the United Kingdom (London). Several of our sub-processors (notably OpenAI, Anthropic, Google, Meta, Twilio, Microsoft, Xero and Folk) process personal data in jurisdictions outside the United Kingdom and the European Economic Area, including the United States (and, for Xero, Australia and New Zealand).

Where personal data is transferred outside the UK, we rely on one of the following safeguards mandated by UK GDPR Article 46:

- the UK International Data Transfer Agreement (IDTA), or the EU Standard Contractual Clauses with the UK Addendum, as included in each sub-processor's data processing terms;
- an adequacy decision issued by the UK Secretary of State, where one applies (for example, the UK-US Data Bridge for transfers to certified US recipients);
- explicit user consent, where neither of the above applies and consent is freely given.

A copy of the relevant transfer agreement is available on request from privacy@tyten.ai.

13. Automated Decision-Making and AI

Tyten uses third-party Large Language Models (currently OpenAI's GPT family, Anthropic's Claude family, and Google's Gemini family) to generate suggested tools, probable causes, and diagnostic steps for technicians, and within our automated workflows to classify documents and emails and extract data from them. These suggestions are decision-support, not automated decisions: a human technician always reviews and applies them. We do not use AI to take decisions that have legal or similarly significant effects on individuals.

For technician guidance, we send the relevant work-order text and (where attached) photographs to the AI provider's API. We do not include the technician's name, email, or any account identifier in the prompt, unless the user has typed one into the

work-order description themselves. Documents and emails processed in our automated workflows can contain names and contact details, and these reach the AI provider as part of that content. AI providers process this content under their own data-processing terms and do not train their public models on it.

Users have the right to obtain human review of any AI-generated guidance by contacting privacy@tyten.ai.

14. Contact

For any questions, concerns, or requests relating to this Privacy Policy or our processing of personal data, please contact:

Email: privacy@tyten.ai

Post: Tyten Technologies Limited, 25 Eccleston Place, London, England, SW1W 9NF

This policy supersedes all prior versions.