SchoolGo · Zinteli Ltd

Privacy Policy

Last updated 21 November 2026

Applies to: SchoolGo version 1.0 for iOS, iPadOS and Android, and the SchoolGo web app

Who we are

SchoolGo is published by Zinteli. For any question about this policy or your data, write to **info@zinteli.com**. This policy describes what the app and its server do; it is not a statement about anything else Zinteli operates.

The short version

- SchoolGo is used by schools and transport providers to run the school journey. The records they keep - about pupils, their parents and carers, drivers and staff - are held on our server for that organisation and shown only to its members whose role allows.
- On a phone, those records are also kept on the phone, in a database encrypted with a key held on that phone. The web app keeps none of them after you close it.
- Documents you photograph or import - licences, certificates, forms - stay on the device you kept them on. We never receive them unless you share one yourself.
- If you turn backups on, the phone app copies its records and your display settings to **your own** Google Drive, OneDrive or iCloud Drive, encrypted with a passphrase only you know. We never receive a backup and cannot open one.
- We collect **no** advertising identifier and no browsing history, and no location except a driver's phone's during a trip (4c). We do not track you across other apps or websites.
- Crash reports, diagnostics and feature-usage events are sent **only if you turn them on**. The setting starts undecided, which means off.
- Creating an account requires an email address. That is the only directly identifying information we hold.

What we collect, and why

1. Your email address - required for an account

Why: to sign you in, to let you reset a password, and to verify the address.
Linked to your identity: **yes**, because an account without an identity cannot be signed in to.
Stored: on our server, hashed and salted password derivative (never the password itself). When confirmation by email is switched on, your address and that password derivative wait on our server until you open the link we email you; only then do they become your account, and if you never open it, nothing does. While it is switched off, the account is created at once. If you register or sign in with Google or Apple, we receive your email address from them - and from Apple, the name you choose to share - and no password is created.

2. Crash and diagnostic data - optional

Why: to find and fix defects.
What: crash logs, stack traces, the app version, the operating-system version and the device model.
Linked to your identity: **no**. The record carries a random correlation identifier, not your account identifier.
Stored: on our server for the retention period, keyed by a fingerprint of the crash so repeats group together.

3. Product interaction - optional

Why: to know which screens are used, so effort goes where it is needed.
What: the names of screens opened and features used. Names come from a fixed catalogue of ten event names built into the app; no free text is possible, and no event carries content you typed.
Linked to your identity: **no**.
Stored: on our server for the retention period.

4. The transport records

Why: to plan and run the school journey, and to keep the people responsible for each child informed.
What: schools; children's names, dates of birth, schools, pick-up and drop-off places, and - only where a parent or school records them - allergies, medical and care notes and emergency contacts; parents' and guardians' names, relationships, phone numbers and email addresses, and what each guardian may see; drivers' names, contact details, licence and background-check details, vehicles and seats; which schools a driver serves and which driver takes which child; trips, who was on board and when, absence reports and announcements.
Who enters it: schools about themselves; drivers about themselves and their vehicles; parents about themselves, their children and the other guardians they add.
Who sees it: only the people a record concerns. A school sees its pupils, the drivers it approved and the trips that carry its pupils; a driver sees the schools they applied to, the children they carry and their own trips; a parent or guardian sees their own children - within the access the child's primary guardian gave them - and those children's drivers and trips. Nobody sees another family's children.
Stored: on our server, with children's details, addresses, notes, contact details, photos, documents and messages encrypted before they reach the database; on each phone that is signed in, encrypted; in the web app only for as long as the page is open. Transmitted over TLS.
Our role: for these records, the organisation is the data controller and we process them on its behalf.

4a. Documents you keep

Photos and files you keep in the app's Documents area are encrypted and stored only on the device where you kept them. They are sent anywhere only when you share or download one. We never receive them.

4c. A driver's location, during a trip only

Why: so the families and the school on a trip can see the vehicle approach, with an arrival estimate, and so a pick-up or drop-off records where it happened.
What: the driver's phone's position, speed and direction, about every 10 seconds, from the moment the driver starts a trip (or a scheduled run starts it) until it ends - also while the app is in the background or closed. Android shows a notification and iOS the location indicator for the whole time.

Nothing is recorded outside a trip, and nobody but the driver sees a position outside a running trip. Who sees it: the trip's driver; while it runs, the school's staff and the guardians of a child on it who may see the live location. Linked to the driver's identity: **yes**.

4d. Photos and drivers' documents

A child's photo, added by their parent so the driver recognises the child, is seen by the child's guardians, drivers and school. A driver's photo ID, licence, insurance, vehicle registration and background check, added by the driver, are seen by the driver and the schools reviewing them. Both are encrypted on our server.

4e. Messages, notifications and emergencies

Messages between a parent and their child's driver, or a driver and a school; the notifications we send you about trips, pick-ups, requests, announcements and payments; and emergencies a driver raises, with the position at that moment. Messages are seen by the two sides of the conversation only. To deliver notifications to a closed app we keep a push token for each phone you sign in on, and pass the notification's title and text to Google (Android) or Apple (iOS) for delivery.

4f. Drivers' subscriptions

When payments are switched on, a driver subscribes on Stripe's own pages. Stripe receives the card and billing details; we receive and keep only the subscription's status, plan and dates. Schools and parents never pay.

4g. A record of changes

Who changed a trip, a child's record, a driver's approval, a request, an announcement, a message's existence or an emergency, when, from which address and device. The school sees the record for its own pupils and drivers; it cannot be edited. The content of messages is not copied into it.

4h. Backups - only if you turn them on (phone app only)

A backup is an encrypted copy of the records on your phone, the changes it has not sent yet, and your display and accessibility settings (theme, language, text size, contrast, motion). It never includes your sign-in, the documents you keep, or diagnostics. The phone encrypts it with a key made from a passphrase you choose, and saves it in a private folder of the storage you connect - your Google Drive, OneDrive or iCloud Drive - which only SchoolGo can see there. We do not keep your passphrase; if you lose it, nobody - including us - can open your backups. To connect Google Drive or OneDrive, you approve SchoolGo on Google's or Microsoft's own page; our server completes that step, because it needs our app's secret, and passes the resulting access to your phone without keeping it. That access reaches only SchoolGo's own folder, and you can withdraw it at any time in your Google or Microsoft account, or turn it off in the app. Automatic backups, if you choose them, keep the key - never the passphrase - in your phone's secure storage until you turn them off. The backups themselves stay in your storage until you delete them.

4b. Cookies and browser storage (web app only)

The web app uses two strictly necessary cookies, both readable only by our server: one holds your sign-in for a few minutes at a time, the other renews it. With **Remember me** ticked the second is kept for up to 400 days from the last time you open the app, so you stay signed in until you sign out;

unticked, both end when the browser closes. It also keeps your preferences (language, theme) and a random identifier for the browser in the browser's local storage, and the documents you keep in the browser's own encrypted storage. There are no advertising or third-party cookies, and nothing is used to track you.

5. Feedback you send us - only if you send it

Contains your email address, the message you write, and - only if you tick the box - a diagnostics attachment. You choose whether the box is ticked.

What we do not collect

Anybody's location outside a trip, and a parent's or school's location at all. Contacts. Calendar. Microphone. Advertising identifiers. Browsing history. Card details. Anything used to track you across other apps or websites. The documents you keep in the Documents area stay on your device (4a).

The Android build declares: `INTERNET` and `ACCESS_NETWORK_STATE`; `CAMERA`, used only when you choose to take a photo; `ACCESS_FINE_LOCATION`, `ACCESS_COARSE_LOCATION`, `ACCESS_BACKGROUND_LOCATION`, `FOREGROUND_SERVICE` and `FOREGROUND_SERVICE_LOCATION`, used only by a driver during a trip (4c); `POST_NOTIFICATIONS`, to show notifications; and `RECEIVE_BOOT_COMPLETED`, `WAKE_LOCK` and `SCHEDULE_EXACT_ALARM`, so a trip in progress or a scheduled run carries on after a restart. The iOS build asks for location (while in use and always, for drivers during trips), the camera, the photo library and notifications, declares no tracking domains and does not enable tracking.

Consent, and changing your mind

The first time the app can collect diagnostics, it asks. Until you answer, records are kept on your device in a quarantined area and **nothing is transmitted**. Three consequences, all deliberate:

- If you allow it later, the quarantined records are sent.
- If you refuse, they are never sent, and they are eventually discarded.
- If you allow it and later turn it off, transmission stops immediately and anything still waiting is deleted.

You can change the decision at any time in **Settings > Privacy**.

Who we share data with

Nobody, for their own purposes. There is no analytics provider, no crash-reporting service and no advertising network. Besides our own API, the app talks to:

- **Google (Firebase Cloud Messaging) and Apple (APNs)**, which deliver notifications to a closed app. They receive the phone's push token and each notification's title and text. On Android the app includes Google's Firebase Messaging library for this, which registers the installation with Google.
- **Stripe**, for drivers only, when payments are on (4f).
- **The map's tile server** - OpenStreetMap's by default - which receives your address and the map area you look at when a trip map loads, as any website you visit would.

- **Google, Apple or Microsoft**, if you choose to sign in with them, whose sign-in page receives only what you give it there.
- **Your own Google Drive, OneDrive or iCloud Drive**, if you turn on backups (4h). They store the encrypted backup for you and cannot read it; it is your storage, under your account with them.

Our hosting provider processes data on our behalf and is bound by contract to do only that. Data may be disclosed if we are legally compelled, and we will tell you unless we are prohibited from doing so.

How long we keep it

Data	Retention (configured)
Crash and diagnostic records	90 days
Product interaction records	365 days
Your account and content	Erased immediately on in-app deletion; the anonymous record is kept for 30 days
Feedback you send	730 days (24 months)
Your sign-in (a session record on our server, and on a phone a copy in the app's encrypted database)	Until you sign out, reset your password or delete the account - a sign-in no longer runs out on its own
Revoked sign-in session records	90 days after revocation
A registration whose confirmation link was never opened (its email address and hashed password)	Not yet limited: kept until the same address registers again - see the caveat below
Drivers' positions, messages, notifications and the record of changes	Not yet limited: see the caveat below

> **Operational caveat.** Retention windows are configured in the server's `appsettings.json`, but the scheduled job that applies them is **not implemented** in this release. In practice records are currently deleted only when an operator runs the purge manually. This policy will be corrected to a shorter, firm commitment once the job exists - and the job's absence is a defect we are tracking, not a term of this policy. This caveat applies to the retained account row left behind by an in-app deletion as well: the personal data in it is erased immediately, and the anonymous row itself is cleared when the job exists.

Your rights

You have the right to access, correct, export and delete your data, and to object to processing based on legitimate interests. Write to **info@zinteli.com** and we will respond within 30 days.

Deleting your account. You can delete your account in the app: open **Settings**, choose the **Account** tab, enter your password - or, if you sign in with Google or Apple, your email address - and tap **Delete account**. We confirm first, because the action cannot be undone. Without the app, follow the steps at https://workflowdynamix-002-site9.dtempurl.com/account-deletion/.

When you confirm:

- Your profile and everything synced to your account stop being accessible **immediately**; you are signed out on every device and your sessions are revoked.
- Your personal details are **erased at once** - your email address, display name and password are overwritten with empty values or a non-routable placeholder.
- Data stored on the device you deleted from is removed as part of the same flow.

The anonymous record that remains is kept for 30 days so that the deletion can be audited, then removed. As the operational caveat above records, the job that performs that final removal is not yet implemented; until it runs, the remaining record contains no personal data.

You can also write to **info@zinteli.com** and we will carry out the deletion for you. Diagnostic records already sent cannot be re-associated with you because they were never linked to your identity in the first place.

Data portability. Ask, and we will export your account data as JSON.

Complaining. If our answer does not satisfy you, you can complain to your local data-protection supervisory authority. In the United Kingdom that is the Information Commissioner's Office (ico.org.uk).

Where data is processed

Our servers and the database are hosted in the European Union. If you use the app from outside the EU, your data is transferred to the EU and processed there. The transfer relies on the European Commission's Standard Contractual Clauses where required.

Security

Passwords are stored as a salted hash produced by an adaptive algorithm, never in reversible form. The pass the app shows our server with each request is a short-lived signed credential that renews itself; the sign-in behind it lasts until you sign out. On a phone, the records the app keeps - your sign-in included - are in a database encrypted with AES-256, and the documents you keep are encrypted with AES-GCM, under keys generated at random on the device; the keys are protected by the platform keystore and never leave it. Transport is TLS with the server's certificate validated.

No system is perfectly secure. If a breach affects your data we will notify you and the relevant authority as the law requires.

Children

The app is not directed at children: its users are school and transport staff, drivers, and parents and carers, and an account is for an adult. It does hold information **about** children - the pupils whose journeys it organises - entered by their school or transport provider, which decides what is recorded and is responsible for having a lawful basis to do so. A parent can see and report on only their own children. If you believe a child has created an account, contact us and we will remove it.

Changes to this policy

We will publish a new version here and update the date at the top. A material change will be announced in the app before it takes effect. Continued use after that is acceptance.

Contact

info@zinteli.com
