PRIVACY POLICY

360Nav Pos and Nav360 HR (including Clokd and Clokd Kiosk)

360 NAV TECHNOLOGIES LTD, company number 17447415

Registered office: 9b The Broadway, Woodford Green, England, IG8 0HL

Website: 360navtech.com Email: hello@360navtech.com

Version 2.0, last updated: 10 October 2026

This Privacy Policy explains how 360 NAV TECHNOLOGIES LTD ("we", "us") uses personal data in connection with our website and our products: 360Nav Pos (till and point-of-sale software) and Nav360 HR (HR, rota, time and attendance software), which includes the Nav360 HR web app, Clokd for web, the Clokd employee app and the Clokd Kiosk app (together, the "Services").

We act in two different roles, and this policy is organised around them:

- Section 2: where we are the controller, meaning we decide how personal data is used. This covers our customers' account and billing contacts, website visitors, enquiries and support.
- Section 3: where we are a processor, meaning a business uses our Services to look after the data of its own customers or staff, and we handle that data only on the business's instructions.

1. Who We Are

360 NAV TECHNOLOGIES LTD is a company registered in England and Wales, company number 17447415, registered office 9b The Broadway, Woodford Green, England, IG8 0HL. For privacy questions, contact hello@360navtech.com.

2. Data We Control

This covers the businesses that buy or try our Services, the people who administer their accounts, and visitors to our website. It does not cover employee or customer records that a business keeps in the Services (see Section 3).

Data	Why we use it	Lawful basis
Account details: name, work email, role, company name, sign-in records, two-step sign-in settings (including passkeys)	To provide your account and keep it secure	Contract; legitimate interests (security)
Billing: company name and address, VAT number, billing contact, invoices, and the number of active employees counted each day. Card details are held by Stripe; we see only the card brand and last four digits	To bill for the Services	Contract; legal obligation (tax records)
Support: what you tell us, and anything we need to look at to help you. If you ask us for "view as" support access, a record of the request, your approval and what was viewed	To answer support requests	Contract; legitimate interests
Demo bookings and enquiries	To reply and arrange a demo	Legitimate interests; steps before a contract
Website and app service data: pages visited, device and browser, approximate location	To run, secure and improve the website and Services	Legitimate interests; consent for non-essential cookies

from IP address; technical error reports from our systems (no request contents, cookies, or screenshots)		
Marketing emails	Product news	Consent, or legitimate interests for existing business customers (with an unsubscribe link in every email)

Retention

- Account data: while the account is open, then [2 years].
- Billing records and invoices: 6 years after the end of the financial year they relate to (tax law).
- Support conversations: [3 years]. Records of "view as" support access: kept in the customer's audit log for as long as that log is kept.
- Enquiries that do not become customers: [12 months].
- Website analytics: [14 months].
- Backups: deleted data is removed from our backups within 35 days.

3. Data We Process on Behalf of Our Customers

When a business uses our Services, the business is the controller of the personal data in them and we are its processor, under our Data Processing Agreement. We use that data only to provide the Services and as the business instructs.

3.1 Nav360 HR

Employers use Nav360 HR to manage their staff. Depending on which features the employer uses, the information held can include:

- staff details: name, contact details, emergency contacts, job, sites, contract, working hours, pay rates, payslips, National Insurance number, date of birth, home address and bank details;
- rotas, availability, shift swaps, holiday and other leave;
- clock-in and clock-out times, with the location and Wi-Fi network name recorded at the moment of each punch;
- sickness records, fit notes and return-to-work notes (health information, which is special category data) and absence scores such as the Bradford Factor, which are only used to prompt a conversation and never to make an automatic decision;
- Right to Work check details and evidence, including share codes;
- recruitment (applications and CVs from the employer's careers page), documents and e-signatures, training, reviews, goals, HR case records, announcements and anonymous pulse surveys;
- conversations with Nav AI, where the employer has switched it on.

The employer is responsible for telling its staff how their data is used (we give employers a staff privacy notice template and show a short version in Clokd) and for having a lawful basis for each use.

3.2 360Nav Pos

When a business uses 360Nav Pos as its till, the Software may process personal data about that business's own customers and staff (for example, names on orders, loyalty or contact details entered at the till, and staff logins and shift records). Card payments are handled entirely by the business's separate card terminal and payment provider: we do not receive or store card numbers, expiry dates or security codes.

3.3 If you are a member of staff or a customer of one of our business customers

Please direct questions and requests about your data to that business, as it is the controller. We will help the business respond. In Nav360 HR, HR teams can download everything held about a person, and staff can

download their own data from Clokd for web (My profile, Download my data) and update their own contact details.

3.4 Our apps

App	What it uses	What it does not do
Clokd (employee app, Android)	Your name, work email and staff number when you sign in; your phone's location (precise and approximate), read once when you tap Clock in, Clock out or a break, to check you are at work (a clock-in away from the site is flagged for your manager); the name of the Wi-Fi network you are on at that moment, to recognise your workplace's Wi-Fi when GPS is weak indoors; clock-in and clock-out times, breaks, time-off requests and shift swaps; a sickness report and its reason, only if you report sick in the app; bank details, only if you enter them on the Getting started checklist; messages, kudos, review answers, survey answers and questions to Nav AI, only if you use those features; a secure key made on your phone to prove punches came from it, and a notification token; a check from Google that the phone and app are genuine (Play Integrity), if your employer turns it on; and crash reports, which carry no name, email, screenshots or what you typed	Never tracks location in the background (that permission is blocked in the app); does not read your contacts, files, photos or microphone; does not use the advertising ID, show ads or sell data
Clokd Kiosk (shared tablet at a workplace, Android)	The camera, only to read staff QR badges; the staff number, PIN, badge or QR code used to clock in, and the clock-in times; the tablet's name, app version, battery level and number of punches waiting to upload	Does not use location or the microphone. No photos are kept. No face recognition or biometric matching is used.
Clokd for web and the Nav360 HR web app	Your sign-in details and the HR, rota, time, leave, pay and document information your employer holds about you or your team. Strictly necessary cookies keep you signed in	No advertising cookies

3.5 Nav AI

Where an employer has switched on Nav AI, it answers questions and helps with rotas. It looks up only what the person asking is allowed to see, sends the question and those records to our AI supplier (Anthropic) to write an answer, and never makes decisions about anyone: anything it suggests to a manager needs that manager's approval, and it cannot change shifts, pay or records by itself.

3.6 Support access by our staff

Our staff cannot browse customer data. If support needs to see a customer's account, our staff must ask with a reason, an owner at the customer must approve it, and the session is read-only, lasts 30 minutes, shows a banner to everyone at the company and can be ended early by the owner. It is recorded in the customer's audit log.

3.7 Retention of customer data

Each business decides how long it keeps its data. Nav360 HR's default settings, which the business can change within limits, are:

- clock-in locations: removed after 12 months (the business can choose 1 to 72 months); the time of the punch is kept;
- leavers' records: deleted 6 years after leaving (6 to 10 years);
- Right to Work records: deleted 2 years after leaving (2 to 10 years);
- applications from people who were not hired: deleted 6 months after the decision;
- Nav AI conversations: until deleted, or 12 months after the last message.

When a customer's agreement ends, the customer can export its data within the period stated in our Terms and Conditions, after which we delete it, apart from anything we must keep by law. Data that has been deleted is removed from our backups within 35 days.

3.8 Deleting your Clokd account and data

Your Clokd account is set up by your employer, and your employer is responsible for your staff record. You can ask for your account and data to be deleted in any of these ways:

- Ask your employer. Their HR team can delete your account and staff record in Nav360 HR, or export a copy for you first.
- Raise a data request yourself: sign in to Clokd for web at hrm.360navtech.com, open My profile, then Your data, then Ask HR about your data, and choose Have my data deleted.
- Email us at hello@360navtech.com with your name, your employer and the email address you sign in with. We will pass your request to your employer and confirm when it is done.

What is deleted: your Clokd account, sign-in details, the phones registered to you and your notification settings. What may be kept: your employer may need to keep some employment records where the law requires it, for example pay and tax records (6 years) and working-time records (2 years); your employer can tell you what it keeps and why. Deleted data is removed from our backups within 35 days. Signing out of the app or uninstalling it does not delete your account. These steps are also published on our website at 360navtech.com/hr/delete-account.

4. Who We Share Data With

We use the following suppliers to run the Services. Those that handle customers' data are our sub-processors; we give customers notice before adding or replacing one, and a current list is available on request at hello@360navtech.com.

Supplier	What it does	Data and where
Railway	Hosts our systems and databases (including backups)	All customer data, stored in the EU (Amsterdam, Netherlands). Railway is a US company, so its staff may access data from the US for support.
Cloudflare	Security proxy in front of our sites; stores uploaded files	Traffic passes through Cloudflare's network. Uploaded files (payslips, documents, evidence) are encrypted by us before upload and kept in the EU; Cloudflare does not hold the key.
Resend	Sends sign-in links, invitations and notifications	Name, work email and message content. Sent from the EU (Ireland). Never payslips, bank details or identity numbers.
Sentry	Error reports from our systems and apps	Technical data only. Stored in the EU (Frankfurt, Germany).
Google (Firebase Cloud Messaging; Play Integrity)	Push notifications to Clokd; checks a phone is genuine when it clocks in	A device token, notification text, and an integrity result. Global.
Anthropic	Powers Nav AI, where your employer has switched it on	What a person types to Nav AI and the records it looks up for them,

		limited to what that person may see. Never National Insurance numbers, bank details, payslip files, identity documents, or sickness reasons or medical details. United States. Not used to train AI models.
Stripe	Takes payment for our Services	Our customers' company and billing details, and a daily count of active employees. Never staff personal data.

Each business using Nav360 HR can also choose to connect its own tools (for example payroll software, Slack or Microsoft Teams, single sign-on, or Square). Those connections are set up by the business, which decides what is shared and is responsible for them. We share data with our professional advisers, with regulators, courts and law enforcement where the law requires it, and with a buyer or successor if our business is sold or restructured. We do not sell personal data.

5. International Transfers

Customer data is stored in the EU (Amsterdam, Netherlands) and file storage is in the EU. Some of our suppliers are US companies, or may access data from the US for support or operations. Where personal data is transferred outside the UK, we rely on UK adequacy regulations (for the EU), the UK Extension to the EU–US Data Privacy Framework for certified suppliers, or standard contractual clauses with the UK International Data Transfer Addendum.

6. Security

We protect personal data with measures that include:

- encryption of sensitive fields (such as National Insurance numbers, dates of birth, home addresses, bank details and sickness information) and of all stored files, and encryption in transit;
- separation of each customer's data inside the database so one business cannot see another's;
- two-step sign-in for administrators, passkey and single sign-on options, and immediate removal of access for leavers;
- signed clock-in punches, and the ability to remove a lost phone or kiosk so it can no longer clock people in;
- an append-only audit log, including a record of every view of sensitive details by HR, and regular security testing and key rotation.

No system is completely secure, and we cannot guarantee absolute security. If a personal data breach affects customer data, we will tell the customer without undue delay so it can meet its own duties.

7. Your Rights

Subject to applicable exemptions, you can ask us for access to your personal data, correction, deletion, restriction or portability, and you can object to processing based on legitimate interests or to marketing. To exercise these rights over data we control (Section 2), contact hello@360navtech.com. We aim to reply within one month. For data we process on behalf of a customer (Section 3), please contact that customer first. You may complain to the Information Commissioner's Office (ico.org.uk, 0303 123 1113), but we would appreciate the chance to put things right first.

8. Cookies

Our website and apps use strictly necessary cookies (for example to keep you signed in). We only use analytics or marketing cookies with your consent. See our Cookie Policy for details.

9. Children

Our Services are for business use and are not directed at children. We do not knowingly collect personal data from children, and employers are responsible for the lawful employment of any young workers they record in the Services.

10. Changes to This Policy

We may update this policy from time to time. We will post the new version on our website and tell customers by email about significant changes. The "last updated" date above shows when it was last revised.

11. Contact

360 NAV TECHNOLOGIES LTD, 9b The Broadway, Woodford Green, England, IG8 0HL. Email: hello@360navtech.com.