

Privacy Policy

Last updated October 25, 2026 · stationclipboard.com/privacy-policy

Key points

- We never sell personal information, use it for advertising, or run ad trackers or third-party analytics in our products.
- Most information in Station Clipboard belongs to the fire department, EMS agency, or other Organization that uses it. We process it for them, so start with your Organization for requests about it.
- AI features receive only what a request needs. Sparky never reads passwords, face templates, Social Security numbers, or members' medical records.
- Your device's location is read only at the moment you clock in, and only if your Organization turns on clock-in areas. We never track location continuously.
- Face templates, Social Security numbers, and sign-in secrets are encrypted, and face templates are destroyed on a published schedule.
- You can ask to see, correct, or delete your information. Our fillable request form makes it easy.

This summary is for convenience. The full text below is what governs.

This Privacy Policy explains how **Station Automation Solutions LLC** ("we," "us," or "our") collects, uses, shares, and protects information when you use Station Clipboard: stationclipboard.com and its Help Center, the Department Portal, the Command Portal, the Inspection Portal, the mobile and desktop apps, kiosks and station displays, department websites and other public pages that Organizations publish through Station Clipboard, and our support and communications (together, the "Service"). Words like "Organization" and "Customer Data" mean what they mean in our Terms of Service.

Our commitments. We do not sell personal information. We do not use it for targeted advertising or share it for cross-context behavioral advertising. We do not run advertising or third-party analytics trackers on our website or in our products. We do not sell, lease, or trade biometric information. And we do not share mobile phone numbers or text message opt-in consent with third parties for their marketing.

1. Our Role

Information in an Organization's account. Most information in Station Clipboard is put there by or for a fire department, EMS agency, fire marshal's office, district, municipality, company, or other Organization. For that information, the Organization decides what is collected, who may see it, how long it is kept, and how it is used. We process it on the Organization's behalf, as its service provider and processor, under our Terms of Service and Data Processing Addendum. The Organization's own privacy notices and policies also apply.

Information we control. We decide how to handle information we collect for our own purposes, such as contact and demo requests, Help Center and support activity, issue reports and feedback, website visits, account security records, and billing communications with Organizations.

If you are a member of an Organization, an applicant, a resident who subscribed to an Organization's alerts, a business owner, or anyone else whose information an Organization keeps, and you have a question about that information, contact the Organization first. We will help it respond.

2. Information We Collect

What we collect depends on which products and modules an Organization enables and how people use them.

Organization account information

Organization name, ID, and logo; time zone and address; primary contacts and their email addresses and phone numbers; subscription, trial, and billing status; enabled modules and settings.

Accounts and sign-in

- Name, username, email address, phone number, profile photo, role and permissions, station, shift, rank, and account status
- Passwords and kiosk PINs, stored only as one-way hashes
- Two-factor sign-in settings, with authenticator secrets stored encrypted
- Sign-in history: each sign-in, failed attempt, sign-out, password reset, and two-factor event, with the time, the username and Organization ID entered, the network (IP) address, and the browser or device. We also keep the address of each account's most recent sign-in, and links between accounts a person holds in more than one Organization.

- Records of accepting our Terms: the version, product, time, network address, and browser

Records Organizations keep

Depending on the modules enabled, Organizations may keep:

- **Personnel:** roster details, assignments, certifications, emergency contacts, date of birth, and custom fields the Organization defines, such as radio IDs and apparel sizes. An Organization may turn on a Social Security number field, which is stored encrypted (see Section 3).
- **Medical:** immunizations, physicals, and injuries recorded on a member's record, with dates, results, notes, and attached files, and a list of the member's possible cancer and hazardous-materials exposures, worked out from the incident reports of the units the member rode on
- **Time and staffing:** clock-in and clock-out times, the station or job selected, the clock-in method, notes, corrections, and audit history; the device details and location described under "Time Clock location and device details" below; schedules, availability, trades, pickups, time off, and callouts, including callout reasons such as illness or injury
- **Payroll:** pay rules, compensation, tax withholding elections, deductions, garnishments, year-to-date wages, pay statements, and employer tax account numbers
- **Training and Courses:** training events, attendance, hours, certificates and documents, test scores, how much of each video was watched, and attempts to skip ahead
- **Resources, Policies, and acknowledgments:** documents, versions, acknowledgments, and electronic signatures, with the time, network address, and browser
- **Information Requests:** the answers and documents a member sends when an officer asks them to update their record, their typed signature, and the time, network address, and browser they used; for a paper form, photos of the completed pages
- **HR Info:** performance plans, coaching notes, discipline, leave records and supporting documents (which can include medical documentation), legal holds, and a log of who viewed restricted records
- **Recruiting and Onboarding:** application answers, contact details, dates of birth, uploaded identification such as a driver's license, résumés, background check consent and status, interview scores, reference answers, AI-assisted application reviews when the Organization turns them on (see Section 6), onboarding tasks, and logins for outside services the Organization issues to new members (stored encrypted)
- **Checklists, Assets, and Quartermaster:** inspection results, equipment and gear records, sizes, requests, and issue history
- **Chat, Meet, Tickets, and Corrections:** messages (including direct messages), files, reactions, meeting chat and attendance, tickets, and notices and responses
- **Surveys and Elections:** survey answers, named or anonymous; ballots, which are sealed so that no one can see how an individual voted; and the voter roll, which records only whether, and to the hour when, each member voted
- **Credits, Budget, Calendar, Drive, Station Board, and TIFMAS:** the records each module keeps, including TIFMAS crew phone numbers and reimbursement documents

Time Clock location and device details

- **Location at clock-in.** If an Organization turns on clock-in areas, clocking in from the portal or the mobile app asks your device for its location once, at that moment. We store the latitude and longitude, how accurate the device said it was, the nearest clock-in area, your distance from it, and whether you were inside it. Clocking out also asks once, but clocks you out even if no location is available. Station kiosks never ask for location. If you do not allow location, the portal does not clock you in, and an officer can add your shift for you.
- **Device details.** Each clock-in and clock-out made from the portal or the mobile app records the network address, browser, operating system, device model, screen size, time zone, and language of the device used, so that the Organization can verify where a punch came from.
- Officers who can see all time entries can see this information on a map. Members can see it on their own entries.

Incident Command and the Command Portal

- Incidents, units, crews and riding positions, assignments, PAR rounds and results, MAYDAY and other emergency declarations (which can include a member's name, location, and situation), benchmarks, objectives, hazards, resource requests, and the incident log
- Incident locations and the map markers people place, such as the command post and staging
- Preplans, including building details, drawings, files, and emergency contacts such as owners and key holders (names, phone numbers, email addresses)
- Hydrant locations and flow information
- CAD calls received through an Organization's CAD or alerting integration, including the address, call type, units, and coordinates
- Personnel profiles for incident command, such as radio names and qualifications, and on-duty information from the Time Clock and the schedule

Incident Reporting and NERIS

Incident reports, including addresses and coordinates, times, units, crew members' names, the narrative, fire and hazard details, coded medical, casualty, injury, and rescue information (which may include an EMS patient care report number), investigation findings, attachments, review history, and a log of what was sent to NERIS and NERIS's responses. The NERIS section of our Terms of Service explains what is sent to NERIS.

Fire inspections, code enforcement, and the Inspection Portal

- Businesses and properties an Organization inspects: name, address, occupancy and risk class, owner and contact names, phone numbers, email and mailing addresses, business license numbers, websites, and logos (which we may find on the business's own website)
- Inspections, checklists, notes, photos, fees, violations and corrective actions, and the name, title, and drawn signature of the business representative who signs an inspection on site
- Permits and plan reviews, including the applicant's name, company, phone number, and email address
- Code enforcement cases and notices, including the property owner's name and mailing address
- Special events and event plans, including organizers' contact details, staffing, and radio assignments

Public complaints

If an Organization turns on public complaints, anyone can report a fire hazard from its complaint page or a QR code posted at a business, without an account. We collect the complaint type, description, place, and address; answers to the Organization's own questions; up to six photos; your name, phone number, and email address if the Organization asks for them or you choose to give them; and your device's location only if you tap the button to use it. We use your network address to limit abuse. Your contact details are shown only to the Organization's staff who manage complaints, and they are never printed on a notice to the business. A complaint to a public agency may be a public record (see Section 15).

Fire investigations

If an Organization uses Fire Investigations, it may record origin and cause findings; the legal basis for being on the property, such as consent or a warrant; losses, injuries, and deaths; the people involved, such as owners, occupants, witnesses, victims, and suspects, with their names, dates of birth, contact details, and addresses; interviews, including rights advisements, summaries, and transcripts; evidence, chain of custody records, and the signatures of those who handled it; lab requests; referrals to law enforcement or others; and photos, sketches, documents, and audio or video recordings. Photo files keep their original metadata, including the time and GPS location where the camera recorded them, and we store that time and location with the photo. Field notes can be dictated using your browser's built-in speech recognition, which your browser's maker processes under its own policies. Investigations are visible only to the case team and to people the Organization authorizes to see every case.

Department websites

An Organization can publish a public website through Station Clipboard, on our domain or its own. These sites show what the Organization publishes. They set no cookies, run no analytics or scripts, and have no forms; buttons such as "Apply" or "Sign up for alerts" link to pages in the Service. Visitor requests pass through our content delivery network, which receives each visitor's network address and browser details to deliver and protect the site.

Face clock-in (biometric information)

If an Organization enables face clock-in, a member's device turns a camera image into a face template, a set of numbers, and we store that template encrypted. We do not store face photos for clock-in. Our Biometric Information Policy explains how templates are collected, used, protected, kept, and destroyed.

Other location information

- Addresses and coordinates of incidents, preplans, hydrants, stations, businesses, complaints, and investigation scenes
- Your device's location, read once, if you choose "Show my location" on the Command Portal map. It is used in your browser to show where you are and is not sent to us unless you start an incident at that spot.
- Approximate location that can be inferred from a network address

We do not track anyone's location continuously or in the background.

People who are not members

Organizations can collect information from people who are not members, through public pages and links: applicants and their references; residents who subscribe to Community Alerts (name, email address, phone number, topics, areas, language, and a record of their consent including the wording, time, network address, and browser); survey respondents; Meet guests; people answering a Corrections, ticket, or event plan link; people who report a complaint; businesses and their contacts; people involved in a fire investigation; and people who receive calendar shares or emails the Organization sends.

Device, usage, and technical information

- Network address, browser and device type, operating system, app version, and request timestamps
- Push notification tokens and notification preferences
- Security, access, and activity logs
- Error reports captured automatically when something goes wrong, such as the error, the page, and the browser

- Performance measurements, such as response times
- How often each area of the Service is visited and used, and the star ratings and comments members give it when asked
- Whether an onboarding email or a Community Alerts email was opened, and, if an Organization turns it on, which alert links were clicked

Issue reports and support

- **Contact and demo requests:** name, Organization, email address, phone number, role, department details, and your message
- **"Report an issue":** what you write; a screenshot of the page you were on, which you can remove before sending; the page address; your recent clicks and page changes (the names of fields you changed, never what you typed); recent errors and failed requests; your device and browser details; your network address; and recent server log entries for your account. Reports go to our support team, not to your Organization.
- **Support tickets and Help Center feedback** (for which we keep a one-way hash of your network address, not the address itself)

Information from other sources

When an Organization connects an integration, we receive information from it, such as CAD calls from Active911, apparatus checks from PSTrax, shifts from WhenToWork, events from calendar feeds, weather and news, vehicle details from the National Highway Traffic Safety Administration when an investigator looks up a VIN, and the Organization's department, enrollment, and report status from NERIS.

3. Sensitive Information

Some of the information described above is sensitive under privacy laws. We process it only to provide the Service as the Organization directs, to keep it secure, and as the law requires. We do not use it to infer characteristics about anyone, and we do not sell or share it.

KIND	WHERE IT APPEARS	HOW IT IS PROTECTED
Social Security numbers	An optional personnel field an Organization can turn on, and Information Requests made inside the portal	Encrypted with AES-256-GCM; shown only as the last four digits; each full view is logged; never accepted by emailed link or on paper; never sent to an AI provider
Biometric information	Face clock-in templates	Encrypted with AES-256-GCM; never sent to an AI provider or integration; destroyed on the schedule in our Biometric Information Policy
Health information	Medical records, HR leave documentation, incident report injury and patient fields, and callout reasons	Limited to people with the permissions the Organization grants; views of a member's medical record are logged; medical records are never read by Sparky
Precise location	Clock-in areas, photo metadata, and complaints where the reporter shares location	Read only at a single moment, never continuously
Government identification	Driver's licenses and other ID uploaded to Recruiting or Onboarding	Limited to people with Recruiting and Onboarding permissions; never opened by AI application reviews
Account credentials	Passwords, kiosk PINs, and authenticator secrets	Passwords and PINs stored only as one-way hashes; authenticator secrets encrypted
Criminal and investigative information	Fire investigations, including suspects, rights advisements, referrals, and arrests	Visible only to the case team and people authorized to see every case
Information about minors	Cadet, junior, and explorer programs, applications from minors, and people in investigations	The Organization is responsible for any parent or guardian consent (see Section 14)

Health information and HIPAA. We are not a business associate under HIPAA unless we sign a business associate agreement with an Organization. An Organization that is a HIPAA covered entity is responsible for deciding what patient information it enters.

4. Information We Do Not Want

Station Clipboard is not designed to hold, and Organizations should not enter, unless a separate written agreement allows it:

- Full payment card numbers
- Social Security numbers, bank account numbers, or full government identification numbers, except in the fields built for them
- Patient care reports or protected health information beyond what the Incident Reporting and medical record fields ask for
- Criminal justice information that requires CJIS compliance, such as criminal history records from law enforcement systems
- Face photos for clock-in
- Passwords, alarm codes, or lock combinations in notes, messages, or preplans

5. How We Use Information

We use information to:

- Provide, operate, maintain, and improve the Service and the modules and integrations an Organization enables
- Create and manage accounts, sign people in, and enforce roles and permissions
- Send reports to NERIS and data to other systems when an Organization or its users direct us to
- Send transactional email, push notifications, reminders, and alerts
- Keep audit logs for security and accountability
- Provide customer support, investigate issue reports, and fix problems
- Protect against unauthorized access, abuse, fraud, and security incidents
- Produce reports and exports that authorized users request
- Understand which parts of the Service are used and how well they work for people, using usage measurements and ratings
- Respond to contact and demo requests, and manage our relationships with Organizations
- Comply with legal obligations and enforce our agreements

We do not use Customer Data for advertising, and we do not use it to train AI models of our own.

6. AI Features

Some features use a third-party AI provider: currently Google (Gemini), our default, or OpenAI, as listed on our Subprocessors page. We send the provider only what a request needs. Neither provider receives passwords, PINs, face templates, Social Security numbers, or members' medical records from these features.

FEATURE	WHEN IT RUNS	WHAT THE AI PROVIDER RECEIVES
Sparky, our assistant	When a member who is allowed to use it asks something. Sparky is off until it is turned on for an Organization, which chooses which roles may use it and which areas it can reach.	The conversation, attached files, the page and any draft the member has open, the member's name, email, station, and roles, and the records the member is allowed to see that the request needs, such as members, training, schedules, tickets, applications, and incident reports
Sparky web search	When Sparky decides a question needs current public information	A short search query of up to 400 characters, which the provider runs on its own search service. The query is written from the conversation, so it can include words from it.
Recruiting application reviews	When an authorized person asks Sparky to read an application, in an application hub where the Organization has turned it on	The application's answers, eligibility results, references' replies, and up to six documents such as a résumé. The applicant's name, date of birth, contact details, and answers about protected characteristics or criminal history are withheld, and photo IDs are never opened.
Inspection overviews	When an inspection starts, if the Organization turns overviews on. Overviews always use Google Gemini.	The business's name, address, use, and hazards, and its past inspections, violations, permits, and complaint descriptions; never owner contact details or who made a complaint
Fire investigation assistance	When an investigator asks it to sort field notes or describe photos	The field notes for that step, or up to six photos with their notes and metadata
Reading paper Information Requests	When an officer photographs a completed paper form	Photos of the form and the questions on it. Social Security numbers and documents are never collected on paper.
Business card scanning	When someone scans a card to fill in a preplan or business contact	The photo of the card, which we do not store
"Report an issue" summaries	Automatically, when a member reports an issue	The report, the screenshot if the member kept it, and the technical details described in Section 2. The member's name and email are withheld.

- **People decide.** Sparky proposes changes and makes them only after a person confirms. Application reviews, overviews, and investigation suggestions are advice that a person reviews; they do not make decisions. Sparky may save files it creates for the member who asked, and it names conversations automatically.
- **Recruiting.** An application review includes a summary, strengths, concerns, suggested interview questions, and a score out of 100. It is advice to the Organization, which makes every hiring decision and is responsible for any notice the law requires when AI is used to evaluate applicants.
- **Conversations.** We keep Sparky conversations so members can return to them. Our authorized staff may review them to support the Organization and improve Sparky.

- **Provider settings.** Requests to OpenAI are sent with storage turned off. Each provider handles the requests we send under its terms for business customers.

7. How Information Is Shared

We do not sell personal information. We share it only as described here.

Within the Organization

Authorized users see information according to the roles and permissions the Organization sets. Members of one Organization cannot see another Organization's data.

Publicly, when an Organization chooses

Organizations can publish department websites and public pages and links, such as application hubs, Community Alerts sign-up pages, complaint pages, public surveys, event plan links, calendar links, Station Board links, and shared tickets. Information on them can be seen by anyone with the link.

Our public issue board

When you report an issue, its title, category, priority, status, and any public update we write may appear on our public issue board. The title is written for the board, without names or details from your screen. Your name, your description, and your screenshot are never shown there.

With service providers

We use service providers for cloud hosting, databases, file storage, content delivery, email delivery, push notifications, maps and address lookup, weather, AI features, and similar functions. They may use information only to provide their service to us. Our Subprocessors page describes each one, what it does, and what it receives.

With integrations an Organization connects

When an Organization connects a service, such as Active911, PSTrax, WhenToWork, Google Sheets, a weather service, a text messaging account, or a Workflow that calls another system, we exchange the information that connection needs, using the Organization's own account. That service's privacy policy applies to what it receives.

With NERIS

When an Organization's authorized user sends an incident report, incident analysis, or station information to NERIS, we send it to NERIS, which is operated for the U.S. Fire Administration by the Fire Safety Research Institute, part of UL Research Institutes. What is sent is incident-level information; crew names and attachments are not sent. NERIS's own terms and privacy policy govern what it does with the information, and NERIS publishes some approved incident information, including incident type, time, address, and location, on public dashboards.

With public information services

Some features look things up in public services, which receive only what the lookup needs: addresses go to the U.S. Census Bureau geocoder and OpenStreetMap; incident and station locations go to the National Weather Service and Open-Meteo; and VINs go to the National Highway Traffic Safety Administration. When a link is posted in Chat or a business's logo is looked up, our servers visit the linked website, which sees our servers, not you.

With the recipients of messages

Emails, notifications, alerts, calendar shares, event plans, and links go to the people the Organization or its users send them to.

For legal, safety, and security reasons

We may disclose information if the law requires it, such as in response to a subpoena, court order, or warrant, or if we believe disclosure is necessary to protect the rights, safety, or security of people, Organizations, the Service, us, or the public. When the request is for an Organization's Customer Data, we will tell the Organization first unless the law prohibits it, and we will refer the requester to the Organization where we can.

Business transfers

If Station Automation Solutions LLC is involved in a merger, acquisition, financing, reorganization, or sale of assets, information may be transferred as part of that transaction, subject to this Privacy Policy and the Organization's agreements.

Text messaging

Mobile phone numbers and text message opt-in consent are not shared with third parties or affiliates for their marketing or promotional purposes. Text message originator opt-in data and consent will not be shared with any third parties, except the messaging providers that deliver the messages.

8. Cookies, Local Storage, and Tracking

We do not use advertising cookies or third-party analytics on our website or in our products. We use these technologies to make the Service work:

- **Sign-in cookies** keep you signed in to the Department Portal, the Command Portal, the Inspection Portal, the applicant portal, and the Help Center. They expire after about a week without use (two weeks for the Help Center).

- **Browser storage** remembers preferences, such as your theme, table layouts, your Organization ID on a sign-in screen, map views, and your department's usual map area, and holds checklist results entered offline until they are saved.
- **Email open tracking.** Onboarding emails and Community Alerts emails can contain a small image that tells the Organization whether the email was opened. Community Alerts link tracking is off unless the Organization turns it on.

Department websites set no cookies at all.

Some content loads from other services, which receive your network address and browser information when it does:

- Fonts from Google Fonts
- Map tiles and imagery from Esri in the Command Portal and Inspection Portal, and from OpenStreetMap on clock-in area maps
- Weather maps from Windy on Station Board screens
- GIF previews from GIPHY in Chat
- Preview images for links posted in Chat, which load from the linked website
- YouTube videos: Chat uses YouTube's privacy-enhanced mode, but some help videos use standard YouTube embeds, which can set YouTube cookies
- Meet connects participants' browsers directly to each other; a connection service (such as Google's STUN servers) sees participants' network addresses

Because we do not sell or share personal information or track you across websites, a browser's Do Not Track or Global Privacy Control signal does not change how the Service works: there is nothing for it to opt you out of.

9. Mobile and Desktop Apps

Mobile app. The mobile app opens the Department Portal, so the information practices in this Policy apply inside it. The app creates a push notification token so the Service can send you notifications through Expo and Apple's or Google's push services; a notification carries a title, a short preview, and a link. The app asks for permission to send notifications, to use the camera, to save images to your photo library, and to read your location when you clock in where your Organization requires it. It does not read your contacts. Apple and other app stores collect information under their own policies.

Desktop app. The desktop app opens the Department Portal, checks for new notifications every few seconds while you are signed in, and keeps its settings on your computer. It allows the portal to use notifications, your camera and microphone, and your location when a feature asks for them. It starts when you sign in to your computer unless you turn that off. It does not send us usage analytics or crash reports.

Station Clipboard's face clock-in is separate from Apple's Face ID and Android face unlock. We never receive the information your device uses to unlock.

10. Data Security

We use technical and organizational safeguards designed to protect information, including:

- Encryption in transit (HTTPS with HTTP Strict Transport Security) for the Service
- One-way hashing for passwords and kiosk PINs
- Encryption at rest with AES-256-GCM for face templates, Social Security numbers, authenticator secrets, election ballots, Google account tokens, text messaging credentials, and stored outside-service logins
- Role-based permissions and separation of each Organization's data
- Two-factor sign-in, available to every Organization and required before our staff can use database administration tools
- Audit logs, including separate audit trails for payroll, HR, elections, onboarding, NERIS, and our own staff's access
- Rate limits and abuse checks on sign-in and public pages

Our Security page describes these practices in more detail and explains how to report a vulnerability.

Access by our staff. A small number of our authorized staff can access an Organization's account, including by viewing the Service as a particular user, and can use administrative tools that reach the stored data directly. We use this access to provide support, investigate problems, set up or move data at the Organization's request, keep the Service secure, and comply with the law. Staff who use administrative database tools must use two-factor sign-in. We record when our staff enter an Organization's account or sign in as a user, and every change or query they make through our database tools, in our own audit log, which we keep permanently. This access may not appear in the Organization's activity log.

No system is perfectly secure. If we learn of a security incident affecting personal information, we will notify affected Organizations, and individuals and regulators where the law requires, as described in our Data Processing Addendum. Users and Organizations are responsible for strong credentials, careful permissions, and reporting suspected unauthorized access promptly.

11. Data Retention

INFORMATION	HOW LONG WE KEEP IT
Organization records	While the Organization's account is active, unless authorized users delete them sooner. Some modules let Organizations set their own retention, and HR legal holds prevent deletion.
Organization activity log	60 days, except entries marked critical, such as security and permission changes, which are kept for the life of the account
Sign-in events	180 days
Our staff's access log	Permanently, as a security record
Workflow run history	90 days, unless the Organization chooses a period between 7 days and two years
Face templates	Destroyed on the schedule in our Biometric Information Policy: at the latest, 30 days after a member's account is disabled or one year after their last activity
Community Alerts sign-ups	Unconfirmed sign-ups are removed after the confirmation deadline. Consent records are kept while a subscriber is subscribed and as long as the Organization needs them to show consent.
Sparky conversations	While the Organization's account is active
Issue reports and screenshots	Until the issue is resolved and we no longer need them to support the Organization or improve the Service; deleting a report deletes its screenshot
Contact and demo requests	As long as reasonably needed to respond, manage a customer relationship, comply with law, or resolve a dispute
Information sent to NERIS	Kept by NERIS under its own policies

When an Organization's account ends. An Organization can export its records before its account ends. When an account is scheduled for deletion, it goes offline at once and can be restored for 7 days. After that, its records are deleted from our production database. Uploaded files are held in separate file storage and are removed in a separate step that can take longer, and copies in backups are removed as backups are overwritten in their normal cycle. Ask us if you need written confirmation that an Organization's records and files have been deleted.

Organizations are responsible for deciding how long their own records must be kept under public records, employment, payroll, fire service, EMS, and other laws.

12. Your Rights and Choices

Depending on where you live and the laws that apply, you may have the right to:

- Know what personal information is held about you and how it is used, and get a copy in a portable format
- Correct inaccurate information
- Delete personal information
- Withdraw consent, including for face clock-in and text messages
- Opt out of sale, targeted advertising, or profiling that produces legal or similarly significant effects (we do none of these)
- Limit the use of sensitive personal information (we already use it only as Section 3 describes)
- Appeal our decision on your request

How to make a request

- **Information in an Organization's account** (members, applicants, residents, business contacts, and others): the Organization controls this information, so send your request to it. You can also contact us, and we will pass your request to the Organization and help it respond.
- **Information we control:** email hello@stationclipboard.com with the subject line "Privacy Request," call (979) 341-9333, or complete our Privacy Rights Request form and email it to us.
- **Community Alerts subscribers:** use the link in any alert email to change what you receive or unsubscribe, or reply STOP to a text message. See our Text Messaging Terms.

What happens next

- **Verification.** We will verify your identity before acting, usually by confirming information we already hold, such as the email address on the account. We ask only for what verification needs.
- **Authorized agents.** Someone you authorize may make a request for you. We may ask for your signed permission, which the request form includes, and may ask you to confirm your identity directly.

- **Timing.** We will respond within 45 days. If we need more time, up to another 45 days, we will tell you why.
- **Appeals.** If we decline your request, in whole or in part, we will explain why. You may appeal by replying to our answer with the subject line "Privacy Appeal" within 60 days. We will answer your appeal in writing within 60 days and explain the result. If you are not satisfied, you may contact your state's attorney general.
- **No discrimination.** We will not deny you service, charge you a different price, or treat you differently for exercising your rights.

13. State Privacy Disclosures

Some state privacy laws, such as those of California, Colorado, Connecticut, Texas, and Virginia, ask businesses to describe their practices in particular terms. This section does that. Where we process information for an Organization, the Organization's own notices also apply.

Categories of personal information. In the last 12 months, we have collected the categories below, from the sources described in Section 2 (you, your Organization, your devices, and connected services), for the purposes described in Section 5, and disclosed them to the service providers, integrations, and recipients described in Section 7.

CATEGORY	EXAMPLES
Identifiers	Name, username, email address, phone number, postal address, network address, account and device identifiers
Customer records	Signatures, employment records, and, where an Organization collects them, Social Security numbers and identification documents
Protected characteristics	Age or date of birth; health information in medical, leave, and injury records
Commercial information	An Organization's subscription and billing history
Biometric information	Face templates for face clock-in
Internet and network activity	Sign-in history, use of the Service, error reports, and issue report diagnostics
Geolocation	Location at clock-in where an Organization requires it, photo metadata, and addresses
Audio, electronic, and visual information	Profile photos, uploaded photos and recordings, and screenshots in issue reports
Professional and employment information	Rank, assignments, schedules, time, pay, discipline, applications, and references
Education information	Training records, course progress, test scores, and certifications
Inferences	AI application reviews and scores, when an Organization uses them
Sensitive personal information	As listed in Section 3

No sale, no sharing, no profiling. We have not sold personal information or shared it for cross-context behavioral advertising, and we do not knowingly sell or share the personal information of anyone under 16. We do not use personal information for profiling that produces legal or similarly significant effects. AI application reviews are advice to an Organization, which makes the decision. We do not offer financial incentives for personal information.

Retention. Section 11 describes how long we keep each kind of information.

California "Shine the Light." We do not disclose personal information to third parties for their own direct marketing.

Consumer health data. Health information in Station Clipboard is collected and used by Organizations to manage their own personnel and incidents, and we process it only for them. We do not sell it or use it for advertising.

14. Children and Minors

The Service is built for Organizations and their authorized personnel. It is not directed to children under 13, and we do not knowingly collect personal information directly from children under 13.

Some Organizations run cadet, junior, or explorer programs, accept applications from minors, or record minors in incident reports and investigations. The Organization is responsible for age limits and for obtaining any parent or guardian consent the law requires, including before a minor enrolls in face clock-in. If you believe a child under 13 has given us personal information without the required consent, contact us and we will work with the Organization to delete it.

15. Public Agencies and Public Records

Many Organizations that use Station Clipboard are public agencies subject to public records, open meetings, and records retention laws. Information in their accounts, including complaints, inspection records, and investigation files, may be a public record. Each Organization is responsible for deciding what must be kept, disclosed, withheld, exported, or deleted under the laws that apply to it. If we receive a public records request for an Organization's information, we refer the requester to the Organization.

16. Where Information Is Processed

Station Clipboard is operated from the United States and is intended for Organizations in the United States. Information in Organizations' accounts is stored in the United States. A few providers that deliver content to your browser, such as weather maps on Station Board screens, may be located in other countries; they are listed on our Subprocessors page.

17. Changes to This Privacy Policy

We may update this Privacy Policy as our products, practices, or legal obligations change. When we do, we will update the "Last updated" date. We will tell Organizations about material changes through the Service, the website, email, or another reasonable method before they take effect when practical. We will not use personal information already collected in a materially different way without giving notice and, where the law requires, getting consent.

18. Contact Us

For privacy questions or requests, contact:

Station Automation Solutions LLC, owner and operator of Station Clipboard
Houston, Texas
Email: hello@stationclipboard.com (subject line "Privacy Request")
Phone: (979) 341-9333

If you are a member of an Organization, also contact your Organization's administrator about your department account or records.

Privacy Policy · Last updated October 25, 2026

Questions about this document: hello@stationclipboard.com or (979) 341-9333. Every legal document and fillable form is in the Legal Center.