

SECURITY AND DATA OVERVIEW

How Duty Line Training Systems handles data.

For information governance, IT security and data protection teams. It describes the software as it works today; where a choice is yours, it says so.

At a glance

Hosting	On infrastructure you control: your server, or a cloud account in your name.
Training content	Fictional callers. Trainees are asked not to use real names or details of real people in practice.
Recordings	Only with the trainee's consent, which they can withdraw; recording can be switched off for any single call. Deleted automatically after 365 days by default (you set the period).
Who sees recordings	The trainee and coordinators. Coordinators see the people they coordinate.
Wellbeing check-ins	Private to the trainee. A coordinator sees something only when the trainee asks for support.
Sign-in	Accounts by role (admin, coordinator, trainee). Two-factor sign-in can be required for staff or for everyone.
Outside services	Care AI plays the callers; voice and transcription services are your choice, including engines that run on your own servers. Listed in full below.
Records	Sign-ins and administrative actions are logged; finished calls are sealed so later changes can be detected.

Where it runs and what it holds

DLTS is a web application you run on a server you control. Its data lives in one data folder on that server:

- **Accounts:** names, roles, sign-in details and department settings
- **Practice records:** for each practice, the transcript, the caller's lines, what the app showed (cards, call sheet, notes), the score and feedback
- **Recordings** (with consent): the trainee's microphone, and camera on a video practice, and each line the practice caller spoke
- **Wellbeing check-ins:** how a trainee felt after a call, and any request for support
- **Logs:** the audit log (sign-ins, administrative actions) and a log of every voice request
- **Backups:** zip files of the data folder; the newest 14 are kept, with an optional copy to a second location

Who can see what

Role	Can see
Trainee	Their own practice, recordings, feedback and wellbeing check-ins. They can delete their own recordings and check-ins.
Coordinator	The practice and recordings of the people they coordinate; support requests those people choose to send. Watching a call live needs the trainee's agreement on that call.
Administrator	Settings, accounts, departments, the audit log, backups and system health. Can delete recordings.

Outside services, and exactly what each receives

Each service below is optional or has an alternative, except Care AI, which is what plays the practice callers. Keys for each are held in your settings; nothing is sent to a service you have not configured.

Service	What it receives	Alternative or control
Care AI (Anthropic)	The practice conversation as text: the fictional caller's brief and lines, and what the trainee says or types. Used to play the caller, give feedback and suggest replies.	Without Care AI, callers use their pre-written lines instead (less responsive). A monthly budget can stop requests once spent.
ElevenLabs (voices)	The fictional caller's lines as text, to be spoken.	Chatterbox voices on your own server; OpenAI voices; or the browser's built-in voice.
ElevenLabs (transcription)	The trainee's voice as audio, one line at a time, with a short list of words to listen for.	Whisper transcription on your own server: the audio then never leaves it. A daily limit applies.
OpenAI (voices, optional)	The fictional caller's lines as text.	As for ElevenLabs voices.
OpenStreetMap	Map tiles are loaded by the trainee's browser. Address searches and routes for fictional incidents in your area go from the server.	None built in; the map shows only fictional incidents.
Freesound (optional)	Search words for background sounds, when building scenes.	Sounds already saved are reused from your server.

The camera check and face reading on video practice run on your own server, using local models.

Controls

- **Consent:** recording and live observation need the trainee's agreement, which they can withdraw
- **Retention:** recordings are deleted automatically after the period you set; trainees and admins can delete sooner
- **Two-factor sign-in:** off, required for staff (admins and coordinators), or required for everyone
- **Audit log:** sign-ins and administrative actions, with who and when
- **Sealed calls:** every file of a finished call is fingerprinted and the list signed, so any later change can be detected
- **Spend and request logs:** a monthly Care AI budget (optional stop when spent); a log of every voice request

What we recommend you do

- Serve DLTS over HTTPS only (browsers also require it for the microphone)
- Encrypt the disk that holds the data folder, and keep backups somewhere equally protected
- Require two-factor sign-in, at least for staff
- Set the recording retention period to match your policy
- If trainees' voices must not leave your network, choose Whisper transcription and a local voice engine

Limits to be aware of

- The application does not encrypt recordings or the data folder itself: use disk encryption
- Backups are standard zip files and are not encrypted by the application
- Care AI receives what trainees say or type in practice; trainees should not bring real people's details into a practice call
- Sealed calls show that a record has changed; they do not prevent the change

Questions from your information governance or security team are welcome: [SALES EMAIL].