

Confidentiality Policy

Company	URBAN TRANSIT SOLUTIONS LTD
Policy owner	Operations Manager
Version	1.0
Effective date	06.06.2026
Review date	06.06.2027
Approved by	Director

Purpose

This policy protects passenger, client, driver, staff and company information from unnecessary disclosure.

Scope

Applies to staff, drivers, escorts and contractors handling information about passengers, children, adults at risk, schools, councils, NHS bodies, account clients, drivers, staff and company operations.

Passenger information

Passenger names, addresses, schools, appointments, vulnerability, disability, behaviour, medical notes, safeguarding concerns, family details, payment details and journey patterns must be treated as confidential.

Children and adults at risk

Information about children and adults at risk must be shared only through authorised channels and only where needed for safe transport, safeguarding, handover, contract management or lawful reporting.

School/council/NHS data

Contract documents, route lists, passenger lists, school/NHS contacts, council instructions, purchase orders and complaint/incident material must not be shared outside the authorised work chain.

Driver and staff information

Licence, DBS/vetting, complaint, disciplinary, payment, medical or contact information about drivers, escorts and staff must be kept confidential and accessed only by authorised people.

Need-to-know access

Access is based on role. A driver may need passenger pickup details and risk controls, but not full background records. An escort may need communication and safety information, but not unrelated family or payment data.

Drivers, escorts, staff and contractors must not store passenger lists, addresses, school details, medical notes, safeguarding notes or journey details on personal phones longer than necessary for the authorised journey or task.

No gossiping or sharing

Do not discuss passengers, incidents, schools, councils, NHS journeys or staff issues in public, with family/friends, on social media, in driver groups or with unauthorised colleagues.

WhatsApp/email controls

- Use company-approved channels where available.
- Keep messages factual and limited to operational need.

- Where information is shared through authorised WhatsApp, SMS or email channels, only the minimum necessary information should be used and sensitive information should be avoided unless essential for safety.
- Do not send screenshots, photos or passenger lists unless authorised.
- Check recipients before sending.
- Report wrong-recipient messages immediately.

Breach consequences

Confidentiality breaches may lead to retraining, warning, removal from route, contract notification, data breach action, referral to TfL or termination of work depending on seriousness.

Responsibilities

Everyone handling company information must protect it. Managers must restrict access and respond to breaches.

Procedure

Use minimum necessary information, approved channels, secure storage and prompt breach reporting.

Records kept

Confidentiality agreements, training records, breach records, corrective actions and review notes.

Review

Reviewed annually and after any serious confidentiality breach.

Approval

Signature

Name

MOHAMOUD MOHAMED

Position

DIRECTOR

Date

06.06.2026