(GDPR) Information Security and Use of Mobile Devices Policy

Purpose

This policy sets out how Peters Travel protects company, passenger, and operational information and ensures the safe and responsible use of mobile devices during Public Service Vehicle (PSV) operations.

The purpose of this policy is to ensure that:

- Information is handled securely and lawfully
- Passenger data and privacy are protected
- Mobile devices are used safely and responsibly
- Distractions and technology-related risks are controlled
- The operator demonstrates good governance in a modern operating environment

This policy supports compliance with:

- The Data Protection Act 2018
- The UK General Data Protection Regulation
- The Road Traffic Act 1988
- The Health and Safety at Work etc. Act 1974
- Traffic Commissioner expectations regarding professionalism and governance

Information security is recognised as an operational and reputational risk, not just an administrative matter.

Scope

This policy applies to:

- All drivers and staff engaged by Peters Travel
- All company-owned or personally owned mobile devices used for work purposes
- All information relating to passengers, journeys, vehicles, or operations

It covers data protection, information handling, and mobile device use during PSV duties.

Principles of Information Security

Peters Travel operates on the following principles:

- Information must be protected from unauthorised access, loss, or misuse
- Personal data must be processed lawfully, fairly, and transparently
- Access to information should be limited to what is necessary
- Mobile devices must not compromise safety or security
- Technology must support operations without introducing unacceptable risk

Information security is treated as a shared responsibility.

Roles and Responsibilities

Operator Licence Holder

The Operator Licence Holder is responsible for:

- Ensuring appropriate information security arrangements are in place
- Supporting compliance with data protection requirements
- Reviewing serious information security incidents
- Ensuring corrective actions are implemented

Transport Manager

The Transport Manager is responsible for:

- Implementing information security controls relevant to operations
- Ensuring drivers understand expectations relating to mobile device use
- Responding to information security incidents
- Escalating serious concerns to the Licence Holder

Drivers and Staff

Drivers and staff are responsible for:

- Handling information responsibly
- Protecting personal data from unauthorised access
- Using mobile devices safely and lawfully
- Reporting information security concerns promptly

Failure to follow this policy may compromise safety or compliance.

Personal Data and Confidential Information

Personal and confidential information includes:

- Passenger names and contact details
- Booking and journey information
- Incident and complaint records
- Driver and staff information

Such information must be:

- Used only for legitimate operational purposes
- Stored securely
- Not shared without authorisation
- Disposed of securely when no longer required

Use of Mobile Devices

Mobile devices include:

- Mobile phones
- Tablets
- Navigation devices
- Any device capable of communication or data storage

Drivers must ensure mobile device use does not compromise safety or compliance.

Mobile Device Use While Driving

- Handheld mobile phone use while driving is strictly prohibited
- Drivers must not text, call, browse, or interact with devices while driving
- Hands-free use is only permitted where lawful and does not distract the driver
- Devices must be set up before journeys commence

Safety takes precedence over communication.

Navigation and Operational Technology

- Navigation systems must be programmed before driving
- Route changes should be made only when safe to do so
- Drivers must not rely solely on technology where it may be inaccurate
- Physical awareness of vehicle dimensions remains essential

Technology supports driving but does not replace driver responsibility.

Photography, Recording, and Social Media

Drivers must not:

- Take photographs or recordings of passengers without consent
- Share images or information relating to passengers or incidents
- Post operational content on social media without authorisation

This protects passenger privacy and the operator's reputation.

Information Security Incidents

Information security incidents may include:

- Loss or theft of devices
- Unauthorised disclosure of information
- Accidental data breaches

All incidents must be reported to the Transport Manager promptly.

Response and Corrective Action

Where an information security incident occurs:

- Immediate steps are taken to limit impact
- Relevant parties are notified where required
- Root causes are identified
- Corrective actions are implemented

Incidents are treated seriously and reviewed proportionately.

Review and Continuous Improvement

This policy is reviewed:

- Annually
- Following information security incidents
- Following changes to legislation or guidance

Information security arrangements will evolve alongside operational needs and technology.

Position: Company Director - Peter's Travel Ltd

Name: Ilyasali Ahmed Patel

27th January 2026.