Vehicle Telematics Policy (Surrey and Sussex) (1233/2026)

Abstract

This policy provides information on the use of telematics fitted to Surrey Police and Sussex Police fleet vehicles.

Policy

1. Introduction

1.1 This policy defines the provision, use, and management of the telematics system fitted in Surrey Police and Sussex Police (hereafter referred to as the Forces) fleet vehicles and the data produced. It should be read in conjunction with the

Driver and Vehicle Management Strategy (DVMS),

Close Circuit Television (CCTV) and telematics,

Mobile Systems Fitted to Police Vehicles ANPR/Video/Speed Units (Surrey and Sussex) (1206) and respective Force Police Driving and Police Vehicle Incident Policies.

2. Scope

2.1 This policy and subsequent procedure detail the use of telematics, telematics data, reports and Driver ID (use, allocation, returning and reporting a loss). It also sets out the intervention procedure to be followed where the telematics data identifies a potential driving risk or issue that requires further investigation or where a driver fails to log in to the telematics without reasonable justification.

3. Policy Statement

3.1 The overarching aim of the Forces is to improve driving standards and efficiency ensuring we have the correct vehicles in the right place to support policing and plan future requirements. In addition, the use of telematics helps reduce the number of Police Vehicle Incidents (PVIs) and organisational costs.

3.2 Introducing the Driver ID element allows for ready identification of drivers and for profiles to be built so good driving can be recognised and proactive intervention taken where risk is identified.

Procedure

1. Responsibilities

1.1 The respective Force Driver Training Teams are the subject matter experts for driving standards.

1.2 The driver / fleet user is responsible for their own driver behaviour and continuous improvement.

1.3 First line supervisors are responsible for the active supervision of the driving and use of vehicles by their team / staff reporting to them.

1.4 Second line and above supervisors / managers are responsible for ensuring that this policy is applied fairly, and driver behaviour and vehicle utilisation is continuously improved.

2. Telematics

2.1 A Telematics system is a device fitted to a vehicle that records and transmits data. It is widely used by industry and the emergency services to monitor and improve driver behaviour, fleet utilisation, and the efficiency of operational deployment.

2.2 Data collected includes:

• The identity of the driver (see below),

• Where and when a vehicle was switched on,

• Time and date of use,

• Vehicle mileage for each journey and accumulated totals,

• Use of Emergency Equipment (siren, blue lights etc.),

• Vehicle technical status (engine faults, battery voltage etc.),

• Manner of driving (speed, acceleration, cornering, braking etc),

• Location, time, and severity of certain events such as acceleration, cornering, and braking,

• Live and historical location and journey tracking,

• Detailed incident recording.

3. Driver Identification (ID)

3.1 Being able to accurately identify a driver's use of a vehicle is a key element of influencing driver behaviour and gaining maximum benefit from the telematics system. This includes improved safety and efficiency, leading to reductions in the number and

severity of Police Vehicle Incidents (PVIs) and quicker investigation of driving incidents. In the future, it should remove the need to complete logbooks for routine journeys, however until further notice logbooks must still be completed. See section 6.4 Vehicle logbooks.

3.2 The telematics system has the capability to log all vehicle activity and use against a unique driver identity.

3.3 This policy requires that where telematics Driver ID is active on a vehicle, the driver must ‘log in’ using their Driver ID before driving the vehicle (See exceptions at sections 6.2 Hot / Fast Changeover and 6.3 Run-Lock below).

3.4 Every driver will in the first instance be provided with a Driver ID fob. This Driver ID is unique to the individual and must not be shared with or be used by other persons. (In the future, other methods of Driver ID may be introduced, e.g., integrated with the new Force identity card or app-based solution).

A very limited number of pool fobs will be made available to some units for occasional use where an immediate issue may be needed. A record of their use must be maintained by that unit, with the vehicle logbook filled out as usual.

3.5 **Issue of Driver ID**

Officers and staff who have an authorisation to drive, irrespective of grade, will be issued with a Driver ID device (usually fob or card) that is uniquely programmed to them. This must be used to ‘log in’ to vehicles. The issuing and control of the device will be managed by Joint Transport Services (JTS). **Driver ID devices must not be passed on or used by other drivers.**

3.6 **Return of Driver ID**

On leaving the Force or no longer being authorised to drive, you are required to return your Driver ID device to JTS. This also includes people who are rejoining the force on a new contract. i.e. retire and rejoin, staff member becoming an officer, officer returning as staff member. Your Driver ID is linked to your employee number which will be different in any of the above scenarios. A change of role or posting within current employment contract does not need a new Driver ID. See JTS How Do I? for guidance.

3.7 **Lost Driver ID**

Should a Driver ID be lost, first contact and report the incident to your supervisor. Then email the JTS Driver and Vehicle Management (DVM) Team ensuring your first line supervisor is copied in) who will log the loss and arrange a replacement.

3.8 **Found Driver ID**

Each Driver ID (Fob) has an identification number, which differs from the unique Driver ID number programmed on to it. This if for security and so that fobs can be reprogrammed and reissued.

Should a Driver ID be found, you can check MINTv4 on the Intranet which now includes Fob ID numbers.

Alternatively, if the ID number is not legible or not on MINT, please contact the JTS DVM Team who hold a record of who the Driver IDs have been issued to, and programming equipment, so it can checked be returned.

3.9 **Defective Driver ID**

For a defective Driver ID, email the JTS DVM Team ensuring your first line supervisor is copied into the email, who will log the fault and issue a replacement.

You should not drive a vehicle equipped with active Driver ID until your lost or defective Driver ID fob has been replaced.

3.10 **Driver ID Reader faults**

Where the ID reader is faulty, for example, not silencing upon presentation of a Driver ID or beeping at random times whilst vehicle is in use, a vehicle defect notification must be completed and submitted to JTS as per usual process.

Neither the telematics unit nor ID reader will have any effect on the safe operation of the vehicle or its equipment.

Consideration however must be given to removing the vehicle from service if there is a persistent beeping from an ID reader fault as it can be distracting for the driver.

4. Telematics Back Office

4.1 The data from the telematics device (vehicle and Driver ID) are securely communicated to the telematics back office, where the data is converted into information and reports regarding the vehicles use. Data will be downloaded via GPRS and stored securely by the contractor for a period of seven years.

4.2 The telematics back office allows authorised users to view this data via a web-based portal for a single vehicle or driver, or groups of vehicles or drivers. It also provides the capability to generate a range of reports to show both driver behaviour and how drivers are using vehicles.

Examples of how these reports will be used include:

• Informing and improving driver standards, recognising good behaviour, and enabling proactive intervention to be taken where risk is identified.

• Improving fleet utilisation through use of live and historical data,

• Reducing fleet operating costs such as accident damage, fuel, and maintenance,

• Supporting investigations both internally and externally, for example, an allegation a driver has used a vehicle outside of their permit authorisation, or a complaint from the public about driving.

• Assisting operational and planning managers to optimise deployment of policing resources. The locating and recovery of vehicles post operations.

Whilst the data is accurate, telematics units are not a Type Approved Device authorised by the Secretary of State for the purpose of excess speed offence prosecutions. However, it can be used in corroboration with other sources i.e. CCTV and is sufficient for internal monitoring and management.

A Data Protection Impact Assessment (DPIA) and an Information Security Risk Assessment has been completed in respect of telemetry use in the Forces fleet.

5. Installation and Provision of Telematics Equipment

5.1 **Telematics Equipment**

JTS are responsible for the provision, installation, and maintenance of all telematics equipment via their approved contractor.

A telematics system / device will be installed in all fleet vehicles except for those agreed by the Driver and Vehicle Management Governance Board where there is a justifiable operational or other reason for it either:

• Not to be fitted,

• Be fitted with telematics but without Driver ID, or

• Other agreed device to monitor driver behaviour is fitted, or• Provision of additional Driver ID's and restriction of access to data in relation to IDs, individual vehicles, or vehicle groups.

6. Use of Telematics Equipped Vehicles

6.1 It is the responsibility of each driver to ensure they are permitted to drive the category of vehicle they are driving, the use of that vehicle, any exemptions, tactics, and any equipment fitted.

When starting a vehicle, the driver must identify themself by presenting their Driver ID to the ID Reader of the telematics system.

If a Driver ID is not presented, the vehicle will continue to emit a repeated beeping noise. Failure to present a Driver ID does not immobilise the vehicle, (this is a safety feature to enable the vehicle to be moved in an emergency) however the journey and all other data will be recorded as usual.

Reports can be produced to show when and where vehicles have been used without a driver being logged in and these may be investigated to ascertain who the driver was and why they did not comply with this policy.

6.2 **End of Journey and Hot / Fast Changeover**

At the end of each journey when the ignition is switched off, the system resets and it will be necessary for the driver to offer the Driver ID again to confirm their identity if prompted. A reset can take up to 30 seconds so a hot or fast changeover of drivers for operational reasons may not register. Where this occurs, drivers must log in at the next opportunity and make a retrospective entry in the vehicle logbook should this happen.

6.3 **Run-Lock**

When 'Run-Lock' is operating, data is being recorded against the driver who identified themselves when starting the vehicle. Where a vehicle is being moved at or from a scene and the driver is different from the original driver, the process at section 6.2 must be followed.

6.4 **Vehicle logbooks**

Vehicle Logbooks still require completion for all journeys, refer to the Police Driving Policy (Surrey and Sussex) (616).

Once the use of Driver ID has become business as usual, a decision will be made and communicated as to the necessity of completion of logbooks for routine journeys for vehicles with active Driver ID.

6.5 **Access to the Telematics information**

Requests for a log in access to the telematics portal are to be sent to JTS. Please see JTS How Do I? Access will be restricted to those roles with a clear business need. All access to the data is auditable.

Different levels of access can be created for different users.

Where a person leaves the Force, JTS will be notified by HR and arrange for removal of access from the system.

Note: The system is only accessible on approved work devices via the Force network or Virtual Private Network (VPN).

7. Telematics Interventions Process

7.1 The telematics system as detailed above generates data and reports that can be used to monitor driver behaviour and vehicle usage. The reports being produced and monitored are directed by the Driver and Vehicle Management Board and Telematics Working Group chaired by the Senior Responsible Officer (SRO) (Assistant Chief Constable (ACC) Operations)

The system and its use have been designed to inform driver and vehicle usage, highlighting good behaviour and encouraging continuous improvement. However, where the telematics data and reports indicate that a driver on that occasion or multiple occasions should be required to account for their driver behaviour, or vehicle usage, the following will apply.

7.2 **Investigation of the event**

For incidents of driver behaviour or vehicle usage that constitute a PVI, the Police Vehicle Incident Policy (Surrey and Sussex) (1232) should be followed (e.g., Driving outside of permit, use of excessive speed, other driver behaviour or vehicle usage that constitutes a significant road risk).

When, where and by whom the vehicle was used may be of benefit for other investigations that do not necessarily constitute a PVI. (e.g., a non-driving complaint about a driver who was using the vehicle, but their identity not known; to trace a driver who may have been a witness from a vehicle known to be in the area at the time of an event; to trace missing vehicle keys).

In such instances these requests will be dealt with on a case-by-case basis with rationale as to why the data is required and either facilitated by the DVM Team or self-serviced by departments that have access to the system.

7.3 **Failure to Log in to the Telematics System**

As set out above, this policy requires that where the telematics system Driver ID is active, the driver must ‘log in’ to the telematics systems using their Driver ID before driving the vehicle (See exceptions at sections 6.2 Hot / Fast Changeover and 6.3 Run-Lock above).

The telematics back office can produce reports where a vehicle is driven without a driver being logged in. This can be individual or grouped data.

Where drives without logins are identified, a requirement may be sent to the relevant supervisor for that vehicle to investigate as to who was driving and why they did not login. This could be established by a physical check of the logbook, vehicle CCTV or other means.

If initial enquiries indicate there was a failure to login without justification, the matter will be referred to Driver Training for review. The outcome will be dependent on several factors which could include if:

• The driver has been previously advised about failing to login.

• It was when the vehicle was used outside of the drivers permit authorisation.

• It was when a PVI or use of concern occurred.

• There was also an omission of entry in the logbook.

In instances where the failure to login is aggravated or repeated, the matter may be escalated to the respective Force Professional Standards Department (PSD).

Team: Joint Transport Service