West Mercia POLICE		POLICY
Security Classification	**OFFICIAL**	
Disclosable under Freedom of Information Act 2000	Yes	

POLICY TITLE	**Telematics**
REFERENCE NUMBER	**WMP193**
Version	**1.1**

POLICY OWNERSHIP	
DIRECTORATE	BUSINESS SERVICES
BUSINESS AREA	TRANSPORT

INITIAL IMPLEMENTATION DATE	**May 2022**
NEXT REVIEW DATE:	**November 2025**
RISK RATING	**LOW**
EQUALITY ANALYSIS	**LOW**

West Mercia Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy.
Please e-mail policiesandprocedures@westmercia.police.uk

1.0 POLICY OUTLINE

The fitting of a full fleet Telematics solution to all Vehicles operated by West Mercia Police is being undertaken to comply with the recommendations of the IPCC report published in July 2007 titled Police Road Traffic Incidents. Recommendation 3 stated:

"*Data recorders should be fitted to all police vehicles and should be regularly checked to ensure they are working accurately, to meet the needs of improving National Police Driving Standards and reduce the number of Police vehicle collision.*"

2.0 PURPOSE OF POLICY

2.1 Telematics is a device fitted to a vehicle that records and transmits that vehicle's activity, location (via GPS), and the identity of the driver for all journeys. Units provide feedback on driver activity against criteria stated in this procedure and the organisations expected driver behaviour within the Safe Driving Policies and their associated procedures. It is the force's legal requirement to maintain vehicle driver records for all journeys.

2.2 This technology is widely used by the insurance industry to monitor driver behaviour, although in the police context, the detail will also be used to monitor fleet utilisation and support efficient operational deployment. In line with the Transport Strategy, this technology will enhance our approach against all aspects of the 5C's framework:

1. **Care** – are staff valuing expensive assets and ensuring we use them to maximum effect to enable protecting the public from harm, professionally and ensuring the fleet do not present a risk to user, workforce or public.
2. **Compliance** – are our staff compiling with the most basic lawful orders including meeting service schedules, MOT, completing accident reporting, logbooks for example. Are they driving to the standard that the organisation and public would expect?
3. **Culture** – is there a healthy and proper culture when allocating vehicles, using the vehicles, refuelling, using peg boards with integrity and ensuring our workforce is able to be mobile safely. 24 hours a day.
4. **Capacity** – are fleet assets in the right place, at the right time and with the right skills to be able to enable service delivery.
5. **Command** – what governance, monitoring and leadership exists to assure and inform 1-4.

The technology will be used to:

- Inform and improve driver safety / standards and enable targeted training and support
- Improve fleet utilisation through live and historical tracking
- Expedite investigations and / or provide corroborative evidence following a concern, complaint, or vehicle incident
- Reduce fleet operating costs such as accident damage (insurance), fuel, and maintenance
- Provide relevant detail to enable operational managers to optimise operational deployment of policing resources

2.3 Data collected includes:

- Driver identity for each journey
- Time and date of use
- Vehicle mileage for each journey and accumulated totals
- Emergency Equipment use (siren, horn etc)
- Vehicle technical status (engine faults etc)
- Driving style (speed, acceleration, braking etc)
- Live and historical location and journey tracking
- Incident detailed recording (IDR/JDR functionality)

2.4 Information is not wholly restricted to the above list. Further detail may be extracted if required, most likely as a result of a collision investigation requirement or Professional Standards investigation.

2.5 Whilst data is very accurate, telematics units are not a Type Approved Device authorised by the Secretary of State for corroborating excess speed offences for the purposes of a prosecution.

2.6 Telematics replaces the requirement to complete mileage details in the vehicle logbook. Drivers should continue to record details of the vehicle check, noting any shortfalls or damage.

2.7 Performance Management of Telematics data will be overseen under the governance of the Strategic Fleet Board.

3.0 IMPLICATIONS of the POLICY

The intention of this policy is to provide clearly defined guidelines for the management of the Telematics system. This policy document includes operating practice, information and details on disclosure of system held data. This policy applies to all employees i.e. police officers, PCSOs, police staff and specials within the force who drive vehicles equipped with telematics or have access to and use associated data.

4.0 PROCEDURE

4.1 <u>Installation and Provision of Telematics Equipment</u>

4.1.1 Telematics is to be installed in all fleet vehicles. Transport Services is responsible for the provision, installation, and maintenance of all telematics equipment via their approved internal staff or third-party contractors. Units will not be fitted or maintained by any other person.

4.1.2 Staff driving fleet vehicles must have a permit issued by Driver Training to drive the category of vehicle they are using. Drivers are issued with a personal Follow Me Printing RFID tab (usually located on the back of their ID card) which is also used to identify the driver to the Telematics system for each journey. The issuing and control of Follow Me Printing RFID tabs is managed by Business Operations (Business Support). Replacement RFID tabs can be requested via MyBOP. Personal issue RFIDs will not be passed to or used by other drivers.

4.2 Use of Telematics Equipped Vehicles

4.2.1 Users are required to undertake the pre-use vehicle checks before driving any fleet vehicle. Drivers must press a Vehicle Check button at the beginning of the journey to show POWDER checks have been completed.

4.2.2 When starting a vehicle, it is a requirement of the driver to identify themselves by presenting a unique identifier to a mounted ID reader. This confirms the driver takes responsibility of the vehicle for the entire journey. A vehicle journey will include any time the engine is running and any movement or repositioning of a vehicle.

4.2.3 Telematics requires a different driver card to those used for ID or building access control i.e. the Follow Me Printing RFID tab. This is for technical and operational security reasons.

4.2.4 If a tab is not presented, the vehicle will emit a loud noise, which will persist until a card is presented. Failure to present a card does not prevent the vehicle from being started or moved, (for operational / safety reasons), however, the event will be picked up in an exception report, requiring a response from the local supervisor as to the reason or justification. It is the responsibility of each driver to ensure they are permitted to drive the relevant category of vehicle they are using. Any lost FMP tabs must be reported to line managers, Digital Services (via MyBOP) and Information Security (via an SIR1) immediately and a replacement requested (via MyBOP).

4.2.5 It is the responsibility of each driver to perform a vehicle check prior to starting the journey i.e. checking the condition of the vehicle and ensuring fluids are topped up, there are no warning lights etc. A ‘Vehicle Check’ button must be pressed prior to commencement of the journey.

4.2.6 It is the responsibility of each driver to check the location of the Harsh Events indicator to enable monitoring throughout the journey.

4.2.7 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 card again to confirm their identity. The reset takes a few seconds, so a fast changeover of drivers for operational deployment may not register. Drivers should keep a note in their pocketbook should this rare occurrence happen.

4.2.8 When Run Lock* is operating (albeit very few of the fleet is still fitted with this) data is being recorded against the driver who identified themselves when starting the vehicle. When the vehicle is being moved at or from a scene and the driver is different from the original driver, the ignition and Run Lock must be turned off and the new driver must go through the engine start-up process to identify themselves to the reader.

4.2.9 Repair and return of faulty units will be managed solely by Transport Services and their contractors.

4.2.10 In all circumstances, management of telematics equipment, passwords, users and information will be for police purposes only.

4.2.11 Interference or tampering with the telematics equipment including RFID reader location sticker or the transmission of data is prohibited.

* Run Lock: A button which allows the engine to continue running when the keys are removed and the car is locked, the purpose being for power management (continual running of ANPR and warning equipment) – this equipment is no longer fitted as kit is now low power consumption.

4.2.12 Integrated front-facing cameras will be installed to operational vehicles including those in CID Reactive, Dogs, Firearms, Patrol, Road Policing and SNT. The retrieval of footage will be outlined in the Police Vehicle Incident procedure.

4.3 RFID (Radio Frequency Identification) tab

4.3.1 In order to drive fleet vehicles, officers and staff will utilise their personal RFID Follow Me Printing tab (usually issued alongside their photo ID card).

4.3.2 Following POWDER checks and pressing the 'Vehicle Check' button, the FMP tab should be presented to the ID reader installed in all police vehicles to confirm the tab owner is the driver.

4.3.3 The tab must be presented individually to the reader without any other cards (such as in a lanyard (recommended), wallet or card holder) to ensure the card's signal is received by the reader.

4.3.4 It is a legal requirement to know who is driving a vehicle so any deliberate avoidance of tab presentation will be considered from a Code of Ethics perspective.

4.3.5 Drivers must continue to report defects and accidents as per existing processes, along with continual completion of the vehicle's logbook i.e. if a defect is discovered during vehicle checks, the relevant online documentation (PVD 1 form) must be completed and submitted to workshops. The vehicle check provides guidance for the next driver of vehicle defects.

4.4 Passwords and User Information

4.4.1 Telematics information is accessed via a secure log-in (Applications). Access is limited to those staff with a direct business need.

4.4.2 Requests for a log-in, together with a business rationale as to why access is required should be sent to Digital Services Systems Administration including an 'approval' email from the Strategic Transport & Fleet Manager; access will be restricted to supervisors and those roles with a clear business need.

4.4.3 The telematics system is delivered via an internet portal. In common with other police sensitive information, details should never be accessible to those without just cause and never to individuals outside the force.

4.4.4 When a user leaves the Force, Systems Administration (Digital Services) will be notified by HR department at the earliest opportunity. Systems Administration will be responsible for deleting users from the system. No other person shall be permitted to set up or amend these details.

4.5 Maintenance of Telematics Units

4.5.1 Transport Services will run reports to show a vehicle's movements over the previous period. Transport Services will check whether a unit is faulty or whether the vehicle has been unused. If a unit is showing as faulty, Transport Services will arrange for the unit to be checked at the workshop and the unit removed and replaced.

4.5.2 If it is evident to a user that a unit is faulty, i.e. the RFID reader is still "pinging" despite an ID being presented, the vehicle must be taken to workshops for the fault to be rectified.

4.6 Telematics Units at Vehicle Dealerships

4.6.1 Vehicles sent to outside repair facilities for warranty work or other repairs will be managed by Transport Services. Where telematics is fitted to such vehicles, a contractor card will be issued for the duration of the repair, if so required for the purposes of road testing.

4.7 Vehicle Mileage Returns and Logbooks

4.7.1 Vehicle logbooks will be kept in the vehicle and should still be completed. This will allow WMP to fall back to record journeys should the telematics system fail.

4.8 Use of and Access to Telematics Data

4.8.1 Telematics units provide real-time and historic detail on any journey undertaken in a fleet vehicle. This includes, date, time, location, mileage, speed and driving standards. Access to this data is managed by the system to ensure data is accessible by those with a justifiable reason to access it.

4.8.2 Transport Services will have access to all data arising from telematics units. This is to enable:

- Management and administration of the telematics system
- Review of vehicle use and utilisation to enable recommendations as to fleet vehicle use and deployment
- To review vehicle use and to manage service maintenance and repairs
- Any other purposes relevant to the safe operations and deployment of the fleet

Access to this detail should be requested via the existing authorised users, depending on context, or via Transport Services. Data can be requested via Transport Services giving details of the reason why it is required.

4.8.3 The dedicated Telematics Strategic Performance & Insight analyst will have access to all data arising from telematics units. This is to enable:

- Production of reports to analyse organisational usage
- Production of agreed reports to other business areas
- Production of ad hoc reports to other business areas

4.8.4 The Strategic Fleet Board is the governing body which will oversee and scrutinise data produced by the Telematics analyst.

4.8.5 LPA/Divisional/Departmental Managers and supervisors will be provided with data relating only to those vehicles and staff for whom they have direct supervisory responsibility on an exception basis. This is to enable:

- Management of vehicle use and utilisation within their area of responsibility
- Management and supervision of drivers / staff within their area of responsibility
- Support the use of resources in the most effective way to meet operational goals

4.8.6 Driver Training Department will have access to driving behaviour data for all staff authorised to drive fleet vehicles. This will enable:

- Remote review of driver behaviours (with and without emergency warning equipment)
- Ability to target and address training requirements, and tailor individual advice and support
- Response and emergency driving will be excluded from driver behaviour feedback although this data will be available to support identified training needs where required

4.8.7 Road Policing will have access to data relevant to a required incident or investigation.

4.8.8 Collision Investigation Teams will have access to data relevant to a required investigation.

4.8.9 Professional Standards Department (PSD) will have access to data relevant to a required investigation i.e. against driver behaviour. The data can be used to assist in investigating instances where Speeding Enforcement Notices have been issues. PSD will not actively search the data for offences committed by officers and staff but where data is analysed for other purposes, and any offences become evident, the data could be passed to the appropriate department / area for further investigation.

4.8.10 Force Operations / Operational Command & Control (OCC) may have access to data relevant to real-time policing requirements.

4.8.11 Business Operations will have access to data to enable the processing of NIPS i.e. investigating whether a police vehicle has justifiably been speeding past an enforcement camera.

4.8.12 Telematics information gathered cannot be used evidentially in a court of law against any driver. However, telematics units automatically self-calibrate and can be re-calibrated if flagged via regular running of a report. This information will be used to assist with improving driver behaviour and utilisation within the criteria mentioned above.

4.8.13 The use of Telematics equipment is considered necessary, reasonable and proportionate, in order to:

- Improve operational efficiency
- Make a positive contribution towards reducing collisions on the road
- Have the potential to support officers and staff relative to complaints against police actions
- Make the best use of resources

4.9 Data Storage and Archive

Telemetry Data

4.9.1 Data will be downloaded via GPRS and stored securely (ISO 27001) by the contractor for a period of six years. Data will be archived on an annual basis so any data requirements beyond this timescale must be requested through Transport Services.

4.9.2 The disclosure principles, contained within policy, which deal with the Attorney General's guidelines on disclosure, must be applied to the data stored. Officers investigating police-owned vehicle collisions will ensure the completed file (which is forwarded for a decision to be made) contains the appropriate information regarding the data limitations and any statement interpreting such data, thus allowing decision makers to be in possession of all information on which to base their decision.

Camera footage

4.9.3 Data will be uploaded from the in-vehicle storage device (DVR) upon request from an authorised officer with system access. Only footage as outlined within the Police Vehicle Incident procedure will be requested i.e. collisions, pursuits and dangerous driving.

4.9.4 Evidential footage will be stored as per MOPI guidelines on the WMP footage solution, currently evidence.com. Unnecessary footage remaining on the UKT cloud solution will be deleted after 30 days.

4.10 Covert / surveillance vehicles

4.10.1 Telematics equipment will be installed into covert / surveillance vehicles to remove the risk of the vehicle being identified as police owned. Drivers will not be required to 'log-in' due to the motion of using the RFID reader. The buzzer will be turned off. Harsh events will be 'softened' on these vehicles due to their expected use outside of blue light activation.

4.10.2 Covert vehicles will be 'hidden' on the system from the majority of users and data will only be made available to WMP upon request in the event of an incident or investigation.

5.0 CONSULTATION

Business Lead Consulted	***Date Consulted***
Helen Broad	Oct 2022

Areas Consulted	***Date Consulted***
Collision Investigation Unit	17/03/22 Project Board
Digital Services	17/03/22 Project Board
Driver Training	17/03/22 Project Board
Fleet Management	17/03/22 Project Board
Force Operations (OCC)	17/03/22 Project Board
Local Policing	17/03/22 Project Board
Professional Standards	17/03/22 Project Board
Strategic Planning & Insight	17/03/22 Project Board
Unison	17/03/22 Project Board
Federation	17/03/22 Project Board
Health & Safety Manager	31/03/22
Strategic Equality & Diversity Advisor	31/03/22
Rick Management and Organisational Learning Officer	31/03/22
Critical Friends Group	04/04/22

6.0 DOCUMENT HISTORY

The history and rationale for change to policy will be recorded using the below chart:

Date	**Author / Reviewer**	**Amendment(s) & Rationale**	**Date of Approval / Adoption**
Apr 2022	Dave Newbold / Ross Walker	New Policy	JNCC Exec Board 10/05/2022
Oct 2022	Ross Walker	Minor amendments re cameras and covert vehicles	Nov 2022

7.0 ASSESSMENT AND ANALYSIS

The Equality Analysis (EA), Health & Safety Assessment (HAS) and Risk Assessment (RA) associated with this document are available on request.

8.0 DATA PROTECTION IMPACT ASSESSMENT

Is a DPIA required? Yes – Approved August 2022.

9.0 MONITORING / EVALUATION

The Monitoring and review of this policy is the responsibility of the policy owner