IN-VEHICLE SAFETY/TELEMATICS MONITORING SYSTEMS

NOVEMBER 2022

CONTENTS PAGE

1. PURPOSE

1.1 The purpose of this policy is to ensure that the vehicle telematics solution used in the Company's commercial vehicles [as defined in the Personal Use of Company Vehicle Policy] and other fleet vehicles, is used appropriately and is compliant with General Data Protection Regulations (GDPR) and the Data Protection Act 2018. Telematics data is personal data within the meaning of the legislation.

1.2 Like many employers, telematics information/data is used within the Company primarily as a Health & Safety tool to encourage safer driving behaviours, reduce accidents and as a tool to aid the efficient scheduling of operational jobs. However, it may be used for a range of additional purposes as set out in this policy.

1.3 Users of the Telematics system should be aware that all activity, system access and use is centrally monitored and reported.

2. SCOPE

2.1 This is a group level policy that applies to all employees of Anglian Water Group Limited, with the exception of Anglian Water (Ireland) Limited and Wave Limited (and their respective subsidiaries).

2.2 This policy does not apply to the following categories of vehicles, which may use different systems and are covered under separate policies:

- WROL Plant Machinery.
- Some plant issued by Fleet Services.

3. STATUS

3.1 The policy is subject to regular review by the Company and is updated as appropriate.

4. POLICY OWNER

4.1 Head of Fleet Services.

5. PRIVACY

5.1 The Company takes the privacy of its employees seriously and has carried out a Privacy Impact Assessment (PIA) and Legitimate Interest Assessment (LIA) on the use of telematic data in company vehicles to ensure:

- appropriate assessments of the privacy risks arising when using telematics data;
- the implementation of appropriate measures and controls to address those risks; and
- an appropriate balance between employee privacy and the legitimate interests of the business.

5.2 The controls and measures identified and implemented as a result of these assessments establish compliance with the principles of GDPR, e.g. the lawful grounds for its use, the purposes for which it can be used and how individual employees are informed. All telematics monitoring in operational vehicles must be processed in accordance with the PIA and this policy.

6. POLICY

6.1 Company commercial vehicles, including company pool cars, are not permitted to be used for any private purpose (please also refer to the Personal Use of Company Vehicles Policy).

6.2 The use of fixed telematics and event recording devices in company vehicles is firmly embedded within the Company. However, company car drivers will have the ability to switch off installed telematics devices when undertaking private mileage.

6.3 The telematics devices installed in company vehicles use third party GPS satellite technology to capture data on the whereabouts of a vehicle and the way in which it is being driven.

6.4 The devices collect real time vehicle location data, speed data, harsh braking and cornering (driving behaviours) as well as vehicle technical information.

6.5 The platform collates collected data and stores it creating a history on the vehicle and its driver.

6.6 Drivers issued with a fob must 'fob in' to the vehicle they are driving on each start. This will ensure that the vehicle journey is allocated to the correct driver.

6.7 Drivers must download the Masternaut Driver mobile application and perform their daily vehicles checks via the app.

6.8 The collection and use of telematics data does not include audio recording data or video/image recording data.

6.9 The telematics devices are functional for 24 hours per day, seven days a week. The data collected is not monitored during collection. However, the collated data will be accessed by the Company for analysis and use.

6.10 All collated data, whether during or outside working hours, may be accessed and further processed.

6.11 <u>Purposes of Processing & Lawful Basis for Processing</u>

6.11.1 The Company needs to collect and use company commercial vehicle tracking data for the following reasons (the legal basis for using the data for the specified reasons is also detailed below):

	Purpose	**Details**	**GDPR Lawful Basis of Processing**
1	To encourage and manage safe driving behaviours, to improve driving skills and behaviours of employees and to	Telematics devices and the supporting system will collect and report on driver behaviours which includes • Excessive speed (in excess of National Road Speed Limit – 70mph)	Necessary for the purposes of the legitimate interests pursued by the Company

	protect the safety of employees and other road users	• Speed in excess of speed limits (e.g. speeding at 35mph in a 30mph zone) • Speed in excess of permitted speed for vehicle category (vehicle type) • Harsh braking • Harsh acceleration • Harsh cornering • Idle time (engine idle) • Completion of a vehicle check via associated mobile application The data reports will be distributed for the purpose of improving driving behaviours by: • The issue of a weekly report to the driver of the vehicle • A monthly scorecard sent to the driver's line manager to aid discussion or support performance management • If required to be used as part of a disciplinary, grievance, PDR or relevant performance management process *Driver event monitoring is required for this purpose.*	
2	To schedule routine jobs efficiently and to ensure a timely, urgent response to emergency jobs and incidents	Telematics data will be used to identify the nearest, available employee resource for appropriate routine job responses and to identify the most appropriate resources to attend emergency incidents or jobs. *Location monitoring is required for this purpose.*	Necessary for the purposes of the legitimate interests pursued by the Company
3	To support the Lone Working Policy and Procedure. Telematics data is used to locate lone workers	Real time location data of vehicles and their allocated driver will be made available to line managers and OMC Managers in order to locate a driver in an emergency situation when the driver is missing or otherwise unaccounted for. The telematics data will support the lone worker system ensuring less vulnerability for our drivers. *Location monitoring is required for this purpose.*	Necessary to protect the vital interests of the data subject

4	For evidential purposes in support of: • The Disciplinary Policy and Procedure • The Grievance Policy and Procedure • The Performance Improvement Policy & Procedure • The investigating and responding to customer complaints • Defending claims against a driver	Telematics may be accessed and used by HR, Line Managers and Business Unit Representatives when necessary to support formal disciplinary (e.g. unauthorised use of a company vehicle or non-worked contracted hours). Grievance proceedings (e.g. to defend or support an allegation of improper conduct made by a work colleague) To drive performance improvement and efficiency. When the data is necessary for a response to a customer complaint or when necessary for defending a claim made against the vehicle driver. *Location monitoring and driver event monitoring is required for this purpose.*	Necessary for the purposes of the legitimate interests pursued by the Company
5	To support vehicle security and the prevention of theft	Telematics data will be used to assist general vehicle security and to support the recovery of a vehicle in the event of theft. *Location monitoring on a 24-hour basis, 7 days a week is required for this purpose.*	Necessary for the purposes of the legitimate interests pursued by the Company
6	To support the Management of Overtime Claims	To the extent that claims cannot be verified by any other reasonable management practices (e.g. reference to site log books, GANNT, OMC, Oracle/Click, Toughbook) and there is reasonable belief that an overtime claim is not accurate, telematics data may be used for the verification of overtime claims. *Location monitoring is required for this purpose.*	Necessary for the purposes of the legitimate interests pursued by the Company
7	To support the Management of Company Vehicles	To the extent that company vehicles cannot be managed by other reasonable management practices and there is a reasonable belief that telematics data will assist with their management, telematics data may be used for the management of company vehicles, e.g. identifying under utilised operational vehicle assets.	Necessary for the purposes of the legitimate interests pursued by the Company

		Location monitoring is required for this purpose.	
8	Data Analytics Business Objects / Power BI	Systems known as Business Objects & Power BI will be used to enhance the reporting functionality set out above in this document and to join Telematics data to other data sets. e.g. time on/at site to optimise business processes. An appropriate amount of historic data will be retained to identify trends and demonstrate business and performance improvements, or otherwise. Access to this source data will be restricted to appropriate users only as per Appendix 1. *Location monitoring and driver event monitoring is required for this purpose.*	Necessary for the purposes of the legitimate interests pursued by the Company
9	System Administration / Supplier Relationship	The system and data are administered and accessed by those set out in Appendix 1. *The Company's Framework Manager is responsible for the supplier relationship.*	Necessary for the purposes of the legitimate interests pursued by the Company
10	Accident/incident support	Data may be used as evidence or support in post-accident investigations.	Necessary for the purposes of the legitimate interests pursued by the Company

6.12 Any purpose for the processing of telematics data not listed at 6.11 above is not permitted unless a full privacy impact assessment has been carried out, reviewed by Legal and approved by the Head of Employee Relations and the Head of Fleet Services or appropriate delegated deputies.

6.13 Telematics data must not be used for the following purposes:

- For the personal interests of employees, e.g. to check the location of a colleague or friend.
- Sharing by line managers with other team members, e.g. the publication or collective presentation of telematics league tables is not permitted.

6.14 The Company uses a third-party data processor to collect and process the telematics data on its behalf; at the time of drafting this policy this is Masternaut, however this may change in future.

6.15 The Company does not share the telematics data with any other organisation save as for any third-party disclosures required by law.

6.16 Other policies relating to this document include:

- The Employee Monitoring Policy.
- Driver Handbook and Fleet Operations Manual.
- Disciplinary Policy & Procedure.
- Performance Improvement Policy & Procedure.
- Grievance Policy & Procedure.
- Data Subject Access Request Procedure.
- Information Security policies.
- Acceptable Use of IT Policy.

7. TELEMATICS SYSTEM USE, ACCESS AND RETENTION

7.1 Access and use of the web-based tracking system and telematics information will be in accordance with GDPR and the Company's Information Security Policies.

7.2 A matrix of users and their access permissions is included in Appendix 1.

7.3 Drivers will be provided with their own driving performance information in report format and via the App.

7.4 Managers will be provided with their own teams driving performance information in scorecard format, and via standard reporting within the online portal.

7.5 All employees who drive company vehicles fitted with telematics devices will be provided with an explanation of how the system will be used and how personal information that is gathered from the system will be processed, including how it is stored securely. Affected employees will be provided with a copy of this policy.

7.6 Telematics data will be available via the third-party supplier's web-based system for the lifecycle of the vehicle.

7.7 At the point that the vehicle and the telematics device is decommissioned the data is permanently destroyed / deleted / eliminated from all systems.

7.8 Interference with telematics devices for the purpose of distorting the information available to the Company will be considered a serious disciplinary offence and will be dealt with under the Company's disciplinary policy.

7.9 An audit log can be produced by the supplier to understand user log in times and certain types of activity, if required as part of a relevant process.

7.10 Telematics data used for analytical purposes will be anonymised fully and stored / used in a manner that is compliant with GDPR.

7.11 The Head of Fleet Services shall be responsible ultimately for all telematics data usage within the organisation.

7.12 The Head of Fleet Services will monitor the logins and appropriate use of the system and make appropriate recommendations if the system is being used in a way that it is not intended to be used.

8. DATA SUBJECT ACCESS REQUESTS AND OTHER REQUESTS REGARDING DATA PROTECTION RIGHTS

8.1 An employee, or third party acting on behalf of the employee, may submit a Data Subject Access Request (DSAR) to obtain a copy of their telematics data.

8.2 The request can be made electronically, via letter or verbally. DSAR requests should be made to line managers or via the DSAR inbox.

8.3 Employees have a number of rights in respect of personal data under the GDPR and Data Protection Act 2018, e.g. the right to be informed, the right of access and the right of rectification. Any requests regarding data protection rights should be made to line managers or via the DSAR inbox.

9. COMPLAINTS PROCEDURE

9.1 In addition to rights given to individuals by way of GDPR and the Data Protection Act 2018 and the right to make a complaint to the Information Commissioner's Office, AWS has its own complaints process for the processing of telematics data. Any individual who believes that the system is being used inappropriately or has a concern regarding data that has been captured has the right to raise a complaint via the Company's Grievance Procedure. During the process, individuals have the right to be represented by a trade union official or colleague.

10. POLICY REVIEW

10.1 The Policy will be reviewed by the Owner on an annual basis.

10.2 Any proposed amendments will be subject to full consultation with the appropriate Trade Unions.

11. FURTHER ASSISTANCE

Please contact Fleet Services for further assistance.

LAST REVIEWED
November 2022

APPENDIX 1

Role	Access Permissions	Access View	Purpose
Operational Managers	• Read only • Vehicles and drivers within line management responsibilities only	• Historical LocationReporting - Driver performance	• Effective and efficient management of team • Support of lone worker system
Drivers	• App access • Emailed reports of driving performance • Own information only	• Historic journeys via App • Reporting – driving performance via App	• Self-management of own driving performance
Fleet Services Managers	• Read only • All vehicles	• Mapping of vehicles • Reporting - Vehicle performance	• Effective and efficient management of fleet • Vehicle security • Maintenance planning
Fleet Services Administrators	• Read write • All vehicles •	• Vehicle and Driver information	• Vehicle location • Vehicle to driver relationship
Senior Operations Manager Operational Control Manager	• Read only • All vehicles	• Mapping of vehicles and the driver	• Support of Lone worker system • Reactive work planning • Incident management
Alarm Handlers	• Read only • All vehicles	• Mapping of vehicles and the driver	• Reactive work planning
Schedulers	• Read only • All relevant vehicles to role by process/geography	• Mapping of vehicles	• Reactive work planning
Masternaut Administrator	• Read write	• Mapping of vehicles • Reporting • Vehicle and Driver information	• System support • Provision of access to system with prior AWS authorisation
Insight Team	• No direct access to portal • Access to source data via Power BI	• Location • Events and status • Time and date stamps	• Business process and performance improvement analysis

APPENDIX 2

Telematics Data – User Code of Practice

Overview:
This Code of Practice ("Code") outlines the principles that govern use of telematics data, its reports and data outputs.

Code of Practice Statement:
We control IT access to information based on business, security and legal requirements. Consequently, access to Masternaut and telematics data has been limited to people across the business who need to:

- Monitor compliance with the General Data Protection Regulation ("GDPR") and other information policies.
- Monitor and manage driving behaviours and performance as defined in the policy.
- Use historic data for analytical purposes.

This Code will support us in protecting the personal data that we need to collect, store and use, and it will support us in responding to the Data Subject's rights as set out in the GDPR.

Each user of Masternaut data system must have read and understood this Code prior to using the application.

We may amend this Code periodically to comply with legal, policy, and functional upgrades to Masternaut (or the telematics service being used at the time), including the addition of new End User Applications.

Aim:
In line with our GDPR policies, this Code of Practice is to provide guidance that will help ensure the security and privacy of employee personal data. This will help us keep data breaches and security risks to a minimum.

Principles:

1. Those with access to the system must use it in a way that is proportionate to achieve their legitimate purposes only.
2. Users must only use their own account / log in details and must not share them.
3. System users must not monitor excessively any employee and must only use the data for the purposes set out in the telematics policy, save for exceptional or emergency circumstances.
    - Users must not use the Masternaut system to search for information about themselves, their family and/or their friends.

Consequences of not adhering to this Code of Practice:
Failure to adhere to the practices set out in this Code may result in the following:

1. We may restrict or terminate user access to the system (with or without notice).
2. Withdrawal or removal of any material downloaded in contravention of this Policy.
3. Where appropriate, disciplinary action may be taken and in the most serious cases, dismissal may be considered.