Vehicle Telematics Policy

Document Status
Draft
Version: V 0.6

Document Change History

<table>
<thead>
<tr>
<th>Initiated by</th>
<th>Date</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alan Whitehead</td>
<td>13th February 2014</td>
<td>Alan Whitehead</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments (i.e. viewed, or reviewed, amended approved by person or committee)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>January 2014</td>
<td>Telematics Group first draft</td>
</tr>
<tr>
<td>V0.2</td>
<td>February</td>
<td>Telematics Group second draft</td>
</tr>
<tr>
<td>V0.3</td>
<td>March 2014</td>
<td>Telematic Group draft for approval</td>
</tr>
<tr>
<td>V0.4</td>
<td>April 2014</td>
<td>Telematic Group draft for approval</td>
</tr>
<tr>
<td>V0.5</td>
<td>May 2014</td>
<td>Telematic Group redraft, following Exec and staffside changes</td>
</tr>
<tr>
<td>V0.6</td>
<td>June 2014</td>
<td>Redraft following Exec and staffside changes</td>
</tr>
<tr>
<td>V0.6</td>
<td>November 2019</td>
<td>Extension to 31st March 2020 approved by MAG</td>
</tr>
</tbody>
</table>
Vehicle Telematics Policy V0.6

<table>
<thead>
<tr>
<th>Dissemination requirements</th>
<th>All managers and staff, via staff bulletins and the intranet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part of Trust's publication scheme</td>
<td>Yes</td>
</tr>
</tbody>
</table>
1.0 Introduction

1.1 The purpose of this policy is to regulate the management, operation and use of the Vehicle Telematic System (VT) fitted to East of England Ambulance Service NHS Trust (EEAST) vehicles.

1.2 Due to the potential for misuse of data generated by the Telematic System, and acknowledging concerns from staffside, this policy is highly restrictive and any deviations from it’s prescribed use may lead to disciplinary action against the individuals accessing or utilising the data outside of this policy.

2.0 Aims

The aims of the Vehicle Telematic system is to:

- Help improve fuel consumption
- Help tailor maintenance and schedule serving of vehicles
- Improve vehicle related performance metrics
- Help inform driver training updates and educational feedback during driver training
- Provide accurate information to third parties when legally required, for example by court order, or under the provision of the Police and Criminal Evidence Act 1984 (PACE). Please refer to section 9 for details.

3.0 Application of This policy

3.1 This Policy applies to all Trust employees employed directly or indirectly by the Trust who are involved in driving Trust vehicles.

4.0 Accountability

4.1 The system and usage will be monitored and reported to SPF monthly, in order to ensure compliance with this policy.

- External requests for individual data with full details of authorisation or refusal (for example police requests, court order)
- Current list of staff and managers given authorisation to access the system.

4.2 The Trust’s CEO has overall legal responsibility for the Trust’s VT.

4.3 The Trust’s Head of Fleet is responsible for maintaining an oversight of the VT, and the procedures supporting their operational use.

4.4 The Trust’s Governance officer is responsible for ensuring compliance with legislation.

4.5 The Head of Fleet is responsible for the downloading, storage and use of any data gathered. It is also the post holder’s responsibility to liaise with the Police or other interested parties if required following such an adverse incident in line with the Trust Policy.

4.6 The Trust’s Head of Fleet is responsible for the approval process and access/use of the system in compliance with this policy and data protection.

4.7 System Users are responsible for complying with the requirements of this policy and associated legal requirements and other relevant policies/procedures.

4.8 The designated third party contractors shall be responsible for the day to day maintenance and servicing of the VT recording system on all vehicles and sites.

4.9 All staff involved in the operation of VT or the monitoring of data have a responsibility to comply with the provisions of the Data protection Act 1998.
4.10 Operating the system will be restricted to only those who have been suitably trained and authorised, a current list of authorised personal will be reported to SPF monthly.

4.11 Any security logins issued to authorised personnel must be kept in safe and secure locations and in compliance with the Trust’s information governance policies.

5.0 System Operations and Data Capture

5.1 Data from this system is not available to Operational managers. Access to data that identifies individuals or incidents is prohibited, unless the Trust is legally required to provide this to third parties. Please refer to section 9. This policy is deliberately restrictive to protect staff against misuse.

5.2 Reports/data will not be generated to look for issues such as speeding, mobilisation times or other operational activities that could be targeted at areas or individuals.

6.0 Access to the Hardware/Software

6.1 It is important that access to, and the disclosure of data to third parties is strictly controlled and documented. This is to ensure that the rights of the individual are maintained and that the chain of evidence remains intact should the data be required for evidential purposes.

6.2 The VT equipment is positioned on board the vehicle that prevents unauthorised access and data can only be viewed if the correct software and appropriate passwords are supplied.

6.3 Access to data and associated equipment is limited to a small number of authorised Trust representatives only.

6.4 No operational staff and managers will have access to VT equipment at any time.

6.5 Employees should not disclose any data or material to anyone outside of EEAST or to any other un-authorised employee without the expressed permission of the Trusts Data Controller. This includes e-mailing data, downloading data, or printing data.

6.6 All data released externally must be documented and approved by the Trusts FOI Manager.

7.0 Maintenance of VT Equipment

7.1 VT should be regularly maintained in line with the service agreement with an approved service provider. Hardware can become ineffective if it is exposed to significant impact or exposed to extreme heat or cold. The Trust must have in place a maintenance log in which to record all maintenance work carried out on the system and its software, and also undertake a regular inspection of the quality of the data being received from the system. The service and work sheets must be obtained and retained for a minimum of 12 months.

8.0 Retaining Information

8.1 Data will be available for on the VT web portal for a period of 12 months. After 12 months the data will be archived for a minimum period of ten years.

8.2 Any data following an investigation which could or will result in litigation must be retained for ten years. Any documents or records relating to any litigation must be retained for a period of ten years as per The NHS Retention Schedule.

9.0 Third party Access to Data

9.1 Police may obtain access to data and or other recording media under the provision of the Police and Criminal Evidence Act 1984 (PACE). Police requesting data from the systems should be made in writing to the Trust’s FOI Manager and should state the purpose of the
request and, as clearly as possible, how failure to disclose would prejudice the stated purpose.

9.2 Access to data and or other recording media may be obtained in connection with civil disputes by court order.

10.0 Signage

10.1 Signs should be placed so that the public and employees are aware that vehicles are fitted with VT and that speed limiters may be operational. The signs should be clearly visible and legible to staff and members of the public.

10.2 The purpose of the signs is to:

• Alert individuals of the VT and speed limiters.
• Promote road safety and good driving practice

10.3 There is no requirement to place signs for vehicles fitted with VT but it is deemed best practice and demonstrates the Trust’s commitment to road safety and efficiencies.

11.0 Disciplinary Procedure

11.1 The information captured by VT cannot be used in any disciplinary investigation against staff.

12.0 Complaints

12.1 Any complaints about this Policy should be addressed to Locality Directors in the first instance.

13. Review

13.0 This policy will be reviewed on a two yearly basis or amended in the light of new employment legislation and/or relevant case law.

14.0 References

Human Rights Act 1998 (Came in to effect in the UK October 2000)
Data Protection Act 1998
Freedom of Information Act 2000
NHS Integrated Information Governance Framework
NHS code of confidentiality
EEAST Records Management Policy
EEAST IT Security Policy