Mobile data devices

Policy

Policy summary

Using mobile data devices removes the need for station based processes. This:
• increases efficiency;
• improves customer service; and
• improves community perception by increasing visibility.

Also, creating and updating records on mobile data devices at that particular time and location improves the accuracy of that information.

This policy procedure relates to all Force issue mobile data devices including personal digital assistants (PDAs), organisers, mobile 'phones, mobile data terminals and other devices of that type, e.g. BlackBerrys and windows mobile devices.

How mobile data devices are used, in conjunction with any data on the Force network, is subject to this policy procedure at all times.

Aims

This policy procedure:

<table>
<thead>
<tr>
<th>No</th>
<th>Aim</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>defines which roles qualify for a mobile data device and what employees are responsible for;</td>
</tr>
<tr>
<td>2</td>
<td>sets out the request, approval and issue process;</td>
</tr>
<tr>
<td>3</td>
<td>details what devices can and must be used for as well as what they should not be used for;</td>
</tr>
<tr>
<td>4</td>
<td>specifies what images can be taken using the camera, where this is enabled, and how these will be managed, checked and audited;</td>
</tr>
<tr>
<td>5</td>
<td>defines what information may be stored on them;</td>
</tr>
<tr>
<td>6</td>
<td>states the level and type of security measures that need to be applied to protect and prevent against unauthorised access or loss of the information;</td>
</tr>
<tr>
<td>7</td>
<td>makes users are aware of what may be claimed for as expenses;</td>
</tr>
<tr>
<td>8</td>
<td>ensures users are aware of what to do in the event of damage or loss;</td>
</tr>
<tr>
<td>9</td>
<td>details how employees performance and use of the devices will be monitored; and</td>
</tr>
<tr>
<td>10</td>
<td>explains the process for transferring and disposing of equipment.</td>
</tr>
</tbody>
</table>

Scope

This policy procedure applies to all police officers, police staff, special constables, police community support officers, contractors, agents
(staff) and third party suppliers who are issued with a Force issue mobile data device.

For officers and staff who have a Force issue BlackBerry which has the camera function enabled, this policy procedure covers overt operational use of the camera. It does not cover the semi-covert, covert or surveillance use. (You should contact the relevant team for further advice on covert use).

Only **current** employees and vetted third party suppliers may be granted access to the Force’s equipment, data and infrastructure.

### Compliance

Employees should acquaint themselves and comply with the following:
- Freedom of Information Act 2000
- Data Protection Act 1998
- Computer Misuse Act 1990
- Official Secrets Act 1989
- Road Vehicles (Construction and Use) (Amendment) (No 4) Regulations 2003
- ACPO Information Systems Community Security Policy (CSP) – standards of maintaining the confidentiality, integrity and availability of information
- ISO/IEC 17799:2005
- NCPE Code of Practice on the Management of Police Information
- NCPE Guidance on the Management of the Police Information (MOPI)
- West Yorkshire Police Protective marking scheme procedure

### Criteria

The Force will prioritise distribution of mobile data devices to constables, sergeants and inspectors in the following policing roles:
- neighbourhood policing;
- response;
- divisional CID or proactive crime; or
- other frontline resources, if deemed appropriate by the senior management team (SMT).

The issue of Force mobile data devices to other employees who are not in a frontline policing role will be at the discretion of SMT. The decision of the SMT will be based on whether the employee’s performance in role would be significantly improved by having a device for use on police business.

### Force undertaking

In all cases, the Force will monitor devices to ensure employees are making the best use of their devices for operational and police business purposes. Performance data will be supplied to line managers to use in their team performance review process and provide improvement plans to employees, where necessary.

The Force, via the IT Department, will:
• distribute devices so that all the frontline staff above are equipped with an appropriate device; and
• redistribute those devices which are not being used optimally or appropriately.

**Employee undertaking**

Employees are accountable for their own actions and their use of the mobile data device at all times. It should be used for police business only, whether on duty or not. This includes all applications on the device, i.e. ‘phone, short message service (SMS), command and control, email, camera etc.

**Staff Associations**

Employees engaged on Police Federation, Trade Union or Superintendents’ Association business may have reason to use Force issue mobile data devices:
• to store Association data; or
• on Association business.

This is accepted and authorised. Information which passes between employees and their representatives is treated as confidential and privileged.

However, it is the responsibility of the Police Federation, Trade Union or Superintendents’ Association member to ensure that the data and costs of using the device can be separately attributed.

**Breaches**

Breaches of this policy procedure may result in the employee being liable to a discipline and or a criminal investigation as follows:

<table>
<thead>
<tr>
<th>By</th>
<th>And</th>
</tr>
</thead>
<tbody>
<tr>
<td>any WYP employee, including agency staff, will be considered a serious disciplinary or legal matter and dealt with accordingly;</td>
<td>access to the WYP network will be terminated until the matter has been investigated.</td>
</tr>
<tr>
<td>a third party supplier employee, will be considered a legal matter and dealt with accordingly;</td>
<td>access to the WYP network will be prohibited until the situation can be brought to a satisfactory conclusion.</td>
</tr>
</tbody>
</table>

All suspected breaches of this policy procedure should be reported to the Force Information Security Officer (ISO) via the Security incident reporting mailbox in line with the Force Security incident reporting procedure.

**Admin**

Last reviewed: March 2012
Scheduled for review: March 2014