Mobile Computing Policy

Issue sheet

<table>
<thead>
<tr>
<th>Document reference</th>
<th>NHSBSAIS004</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document location</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>NHS Business Services Authority Mobile computing policy</td>
</tr>
<tr>
<td>Author</td>
<td>Head of Security and Information Assurance</td>
</tr>
<tr>
<td>Issued to</td>
<td>All staff</td>
</tr>
<tr>
<td>Reason issued</td>
<td>For action</td>
</tr>
<tr>
<td>Last reviewed</td>
<td>December 2017</td>
</tr>
<tr>
<td>Review cycle</td>
<td>Annual</td>
</tr>
<tr>
<td>Date of Equality Assessment</td>
<td>March 2018</td>
</tr>
<tr>
<td>Date of Fraud Review</td>
<td>March 2018</td>
</tr>
</tbody>
</table>

Revision details

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Amended by</th>
<th>Approved by</th>
<th>Details of amendments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial release</td>
<td>21.09.2009</td>
<td>-</td>
<td>IGSG</td>
<td></td>
</tr>
<tr>
<td>V1</td>
<td>09.01.2014</td>
<td>G Wanless</td>
<td>ISF</td>
<td>Identifying who carries out LLM duties</td>
</tr>
<tr>
<td>V2</td>
<td>18.02.2015</td>
<td>G Wanless</td>
<td>ISF</td>
<td>Annual Review</td>
</tr>
<tr>
<td>V3</td>
<td>21.10.2016</td>
<td>C Gooday</td>
<td>ISF</td>
<td>Annual Review</td>
</tr>
<tr>
<td>V4</td>
<td>17/12/2017</td>
<td>ISRS</td>
<td></td>
<td>Reviewed for ISMS update</td>
</tr>
</tbody>
</table>
1. **Policy Summary**
   This policy forms part of the NHSBSA’s initiative to achieve and maintain compliance with ISO 27001 Information Security Management System requirements.

2. **Introduction**

   2.1 This policy applies to the use of all NHS Business Services Authority (NHSBSA) issued mobile computing devices. It is not acceptable for personal mobile computing devices to be connected to any NHSBSA physical network.

   2.2 For the purpose of this policy a mobile computing device (MCD) is defined as any portable electronic device which is capable of capturing, storing, processing, or delivering information electronically. Therefore this includes (but is not restricted to) laptops, tablets, smart phones, digital cameras, USB memory sticks.

3. **Objectives, Key outcomes and Principles**

   3.1 The objective of this policy is to establish the rules for the use of MCDs and their connection to the NHSBSA network. These rules are necessary to preserve the integrity, availability, and confidentiality of NHSBSA’s information.

   3.2 The Key outcome of the policy is to support staff that use MCDs outside of the NHSBSA’s normal business premises, by ensuring they are aware of the information security issues and apply procedures accordingly.

   3.3 This policy applies to all business areas of the NHSBSA.
4. Responsibilities

Overall responsibilities

4.1 Ultimate responsibility for this policy rests with the NHSBSA Leadership Team, but on a day-to-day basis the Information Governance and Security Group (IGSG) and the NHSBSA Head of Security & Information Assurance role within the NHSBSA will be responsible for managing and implementing the policy.

Head of Security & Information Assurance

4.2 HoS&IA responsibilities include:

- ensuring that the appropriate mobile computing policy for the NHSBSA is produced and kept up to date
- assisting the IGSG to monitor the implementation and compliance with this policy across the NHSBSA.

Line managers’ responsibilities

4.3 The use of any MCD outside of the NHSBSA’s normal business premises must be authorised by the relevant line manager.

All staff

4.4 All staff (permanent, temporary or contractor) or agents acting for or on behalf of the NHSBSA have a duty to:

- Ensure that the MCD has a password or PIN enabled that is required to be entered to use the MCD at start-up and after any period of inactivity.
- Protect the MCD from theft. The MCD must never be left unattended, particularly in cars or other easily accessible areas. MCDs must be kept secure and under lock and key when not in use. Care must also be taken in public places as equipment such as MCDs may attract attention.
- Ensure that only authorised (and licensed) software provided by the NHSBSA is loaded onto the MCD.
- Ensure that the MCD is never left in the care of any other person who is not authorised and trusted to protect the information it contains.
- Access the internet only through the NHSBSA network or via other NHSBSA approved connectivity methods such as secure remote access virtual private networks (SVPN). Installation of software provided by Internet Service Providers (ISPs) is strictly prohibited.
- Regularly connect to the NHSBSA network to allow updating of the antivirus checker software and to ensure that backups have been taken.
- Report any loss of a MCD using the NHSBSA Information security incident reporting procedure.
• Return any MCD to the appropriate person i.e. your Line Manager
• Not store any associated PIN numbers or security tokens alongside the MCD.
• Use a purpose made carry case when transporting the MCD outside of the NHSBSA premises.
• Carry MCDs as hand luggage when travelling, where possible.
• Ensure that any MCD is always kept within the environmental ranges detailed with the user guide that accompanies the MCD. This also applies to the media that may also be carried with the MCD (e.g. memory stick or other media).

**Internal audit**

4.5 The NHSBSA will regularly audit its MCD management practices for compliance with this policy.

The audit will:

• identify areas of operation that are covered by the NHSBSA’s policies and identify which procedures and/or guidance should comply to the policy
• follow a mechanism for adapting the policy to cover missing areas if these are critical to the management of mobile computing, and use a subsidiary development plan if there are major changes to be made
• set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance
• highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

5. **Policy framework**

5.1 Only NHSBSA approved MCDs may be used to access NHSBSA information resources.

5.2 MCDs must, be password protected at start-up and after any period of inactivity.

5.3 NHSBSA information which is classified as OFFICIAL-SENSITIVE should not be stored on MCDs. However, in the event that there is no alternative to local storage, all confidential or restricted NHSBSA information must be encrypted using approved encryption.
5.4 NHSBSA information must not be transmitted via wireless connections to or from a MCD unless NHSBSA approved wireless transmission protocols along with approved encryption techniques are utilised.

5.5 All MCD connections made to the NHSBSA environment must be made through the approved, and NHSBSA provided secure virtual private network (SVPN).

5.6 Unattended, MCDs must be physically secure. This means they must be locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

6. **Validity of this policy**

6.1 This policy should be reviewed annually under the authority of the NHSBSA Leadership Team.

6.2 In applying this policy, the NHSBSA will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by theEquality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or political affiliation.

In accordance with our Equality Analysis Procedure, an equality analysis has been undertaken on this policy.

7. **Related policies, standards and procedures.**

This policy should be read in conjunction with the Information security policy (NHSBSAIS001 – Information security policy) and the NHSBSA Information security incident reporting procedure (NHSBSAIS002 - NHSBSA information security incident reporting procedure).

8 **Penalties**

Any Staff who violate this policy may be subject to disciplinary action up to and including dismissal, including criminal prosecution.