Portable Computer Device Policy

Author: Malcolm Flier Head of IT

Executive Lead: Simon Marshall Director of Finance and Information

Status: Approval date: Dec 2015

Ratified by: Information Governance Steering Group

Review date: Dec 2018
<table>
<thead>
<tr>
<th>Issue</th>
<th>Date Issued</th>
<th>Brief Summary of Change</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Nov 08</td>
<td>Amendments to cover Encryption standards</td>
<td>Director of Planning and Information</td>
</tr>
<tr>
<td>2</td>
<td>Nov 09</td>
<td>Amendments to cover non-Trust-owned portable devices</td>
<td>IM&amp;T Strategy Steering Group</td>
</tr>
<tr>
<td>3</td>
<td>Sept 10</td>
<td>Amendments to Departmental names. Addition of Monitoring and Review of Policy</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>4</td>
<td>Dec 12</td>
<td>Amendments to Departmental names and titles. Amendment to Anti-Virus provider</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Nov 2015</td>
<td>Amendment to signatory definition of Remote Access Form approval Added name of new Encryption software Modified to new format</td>
<td></td>
</tr>
</tbody>
</table>

For more information on the status of this document, please contact:

Policy Author          | Malcolm Flier - Head of IT   |
Department/Directorate  | Health Informatics / Finance  |
Date of issue           | Dec 2015                    |
Review due              | Dec 2018                    |
Ratified by             | Information Governance Steering Group |
Audience                | All Staff                   |


Executive summary

Ashford and St Peter’s NHS Trust (ASPH) has a responsibility to ensure that all data stored on its computer systems is appropriate to the needs of the organisation, is securely held, is available in a complete and accurate form when needed and complies with the requirements of the Data Protection Act 1998. The use of portable computer devices increases the risks associated with the secure storage of data. The purpose of this policy is to set out the criteria for the conditions relating to the use of Trust-owned portable computer devices. This policy is a supplementary policy to the Trust Information Security Policy.

For the purpose of this policy, the term “portable device” includes laptops, PDAs, notebooks, tablet PCs and Mobile Clinical Assistants (MCAs) owned by the Trust.
Contents

SECTION ........................................................................ Page

Executive Summary ............................................................... 3
1. Introduction ..................................................................
2. Scope ...........................................................................
3. Purpose ...........................................................................
4. Explanation of terms ..................................................
5. Duties and responsibilities ...........................................
6. Policy ............................................................................
7. Training ...........................................................................
8. Stakeholder engagement and communication ............
9. Approval and ratification ..............................................
10. Dissemination and implementation ............................
11. Review and revision arrangements ...............................
12. Document control and archiving .................................
13. Monitoring compliance with this policy .....................
14. Supporting references / Evidence base ......................

Appendices

Appendix 1 Equality Impact Assessment ..............................
Appendix 2 Checklist for the review and approval of policies
See also: Any relevant trust policies/guidelines or procedures

1. Introduction

This document defines the Portable Computer Device Policy for Ashford & St Peter’s Hospitals NHS Trust and

• Sets out the Trust's policy for the protection of the confidentiality, integrity and availability of the portable devices.
• Establishes the Trust and user responsibilities for portable devices.
• Provides reference to documentation relevant to this policy.

2. Scope

2.1 This guidance is relevant to all staff groups

3. Purpose

3.1 The purpose of this policy is to set out the criteria for the conditions relating to the use of Trust-owned portable computer devices. This policy is a supplementary policy to the Trust Information Security Policy.

For the purpose of this policy, the term “portable device” includes laptops, PDAs, notebooks, tablet PCs and Mobile Clinical Assistants (MCAs) owned by the Trust.

4. Explanation of Terms Used

4.1 PDA - a lightweight consumer electronic device that looks like a hand-held computer but instead performs specific tasks
4.2 MCA- Mobile Clinical Assistants
4.3 RAS - Remote Access Service
4.4 Authorised User: A user who has been authorised to use the portable device by being either the designated owner of the device or a member of staff who has been given permission by the designated owner to use the device.
4.5 Unauthorised software: This is software that has not been authorised for use or installation by the Trust Management or the IT Department
4.6 Unlicensed software: This is software for which the Trust or user does not possess a licence, and therefore has no legal entitlement to use. The use of such software would leave both the trust and the individual open to legal action which could result in a heavy fine, or even imprisonment.

5. Duties and responsibilities

5.1 Users’ Responsibilities

• It is the responsibility of all staff to ensure the confidentiality, availability and integrity of data belonging to ASPH, and to comply with the requirements of the Data Protection Act 1998 and Caldicott recommendations.
• Portable device users must take personal responsibility for the security of the equipment, software and data in their care and abide by the following:
  • Comply with Trust standards on data encryption, ensuring that the portable device is fully encrypted
  • Unauthorised or unlicensed software must not be loaded on portable devices
  • Ensure the portable device is not used by unauthorised persons
  • Take all reasonable steps to ensure that the portable device is not damaged through misuse
  • Portable devices should not be left unattended in public places.
  • When travelling by car, portable devices must be stored securely and left out of sight (e.g. in covered boot) when the car is unattended. The device should be taken indoors overnight wherever possible.
  • Return the portable device to the IT department for regular health checks or when requested
  • Return the portable device before leaving the employment of the Trust
  • Report any possible security breaches (e.g. portable device stolen or misplaced) in line with Trust policy (Incident Form reporting) and advise the IT Department immediately.

5.2 Department Owner Responsibilities
• Where a portable device is not for the sole use of an individual member of staff, but is for departmental use, a department owner for the portable device must be identified.
• The department owner will be responsible for:
  • Complying with Trust standards on data encryption, ensuring that the portable device is fully encrypted and that any encryption passwords are only issued to authorised staff
  • Ensuring that the portable device is issued only to authorised staff
  • Keeping a record of who the portable device is issued to within the department
  • Ensuring staff are aware of the User Responsibilities as detailed above
  • Returning the portable device to the IT Department for regular health checks or when requested

5.3 IT Department Responsibilities
• It is the responsibility of the IT Support department to ensure the correct configuration of portable device devices, including full encryption of the hard drive. The portable device holder is responsible for ensuring the integrity of the configuration (e.g. not installing unauthorised software).
• The IT Support department will be responsible for operating a rolling “health check” programme where portable devices are recalled regularly, during which time the configuration of the portable device will be checked, and any necessary software upgrades completed. The portable device holder must cooperate with the IT Support department and ensure their portable device is checked.

6. Policy
6.1 Ashford and St Peter’s NHS Trust (ASPH) has a responsibility to ensure that all data stored on its computer systems is appropriate to the needs of the organisation, is securely held, is available in a complete and accurate form when needed and complies with the requirements of the Data Protection Act 1998. The use of portable computer devices increases the risks associated with the secure storage of data. Further intranet guidance on PID can be found here: http://trustnet/departments/infogov/Personal%20Data%20Jan%202015.pdf

Remote Access
The Trust offers a Remote Access Service (RAS) to enable users to access the trust network from locations other than that owned by the Trust e.g. home; other NHS sites. This service is available for users with portable devices. A Remote Access application form must be completed, signed by the user’s line manager and approved by the Trust Head of IT. Users must comply with the Remote Access agreement as stated on the application form. The Remote Access form is available through TrustNet.

Person Identifiable Information
Person-identifiable information shall be stored in a portable device only when this is absolutely necessary. Where it is necessary to store such information, the following conditions apply:

- For work involving person-identifiable information, users will be required, wherever possible, to use the Trust network to store data.
- Only the minimum amount of person-identifiable information, necessary for the current purpose, shall be stored. Information deemed to be person-identifiable includes the following:
  - NHS Number
  - Forename
  - Surname
  - Date of Birth
  - Sex
  - Address
  - Postcode
- Person identifiable-information shall be stored only for the time period when it is actively being used.
- It shall be deleted immediately after use.
- Password authentication must be applied.
- Measures shall be taken to maximise the physical security of the portable device.

Encryption
It is Trust policy that all Trust-owned portable devices will be fully encrypted to the Trust’s predefined standards before the device is used to store data. Encryption is applied to the entire hard disk by the IT Support team using the approved Trust encryption software and the authorised user is issued with a password to allow decryption. The password is prompted for when the laptop is first turned on and without it no access is possible. This ensures that should the device be lost or stolen the data would be inaccessible.

Virus Protection
All laptops have the trust approved Anti-Virus software (Sophos) installed at the time they are issued. The anti-virus system must be updated on a regular basis. It is the responsibility of
the laptop holder to monitor this, and to contact the IT Department if they believe this is not occurring. In no circumstances shall the user delete or disable the anti-virus software.

### Use of the Internet

The Ashford and St Peter’s “Internet Usage and Security Policy” applies to Trust portable device computers, whether used on the hospital network, at home or in any other location.

7. **Training**

   No training is required

8. **Stakeholder Engagement and Communication**

   The policy has been written by the Health Informatics Team, ratified by the Information Governance Steering Group. The policy will be available on TrustNet.

   All new staff will be referred to this policy at Induction

9. **Approval and Ratification**

   9.1 Ratification of this policy will be sourced from the Information Governance Steering Group.

10. **Dissemination and Implementation**

   10.1 The policy will be disseminated through the Aspire global email.

   10.2 This policy will be published on the trust intranet and internet sites

11. **Review and Revision Arrangements**

   11.1 This policy will be reviewed by the author every 3 years, or before if necessary.

12. **Document Control and Archiving**

   12.1 This is a trust-wide document and archiving arrangements are managed by the Head of Regulation & Accreditation and Information Content Manager who can be contacted to request master/archived copies.

   12.2 On the internet site, the document will be highlighted as green, when in date, amber 3 months prior to review date, and red if expired

13. **Monitoring compliance with this Policy**

<table>
<thead>
<tr>
<th>Measurable Policy Objective</th>
<th>Monitoring/ Audit method</th>
<th>Frequency of monitoring</th>
<th>Responsibility for performing the monitoring</th>
<th>Monitoring reported to which groups/ committees, inc responsibility for</th>
</tr>
</thead>
</table>

| Section 11 Information & Technology | Current Version is held on the Intranet | First ratified: December 2015 | Review date: December 2018 | Issue 5 | Page 8 of 14 |
This policy will be reviewed by the authors at least annually to ensure that it remains valid and in date

| Compliance audit of sample of policies (including Review History) | Annual | Head of IT | Information Governance Steering Group |

14. **Supporting References / Evidence Base**

14.1 Confidentiality: NHS Code of Practice
14.2 Information Security Management: NHS Code of Practice
APPENDIX 1: EQUALITY IMPACT ASSESSMENT

Equality Impact Assessment Summary

Name and title: Malcolm Flier, Head of IT
Policy: Portable Computer Device Policy

<table>
<thead>
<tr>
<th>Background</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Who was involved in the Equality Impact Assessment</td>
</tr>
</tbody>
</table>

The EIA was performed by the Head of IT

<table>
<thead>
<tr>
<th>Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td>- A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age)</td>
</tr>
<tr>
<td>- The data sources and any other information used</td>
</tr>
<tr>
<td>- The consultation that was carried out (who, why and how?)</td>
</tr>
</tbody>
</table>

The policies were examined and reviewed to ensure that no negative impact on equality would result from the policies.
**Key Findings**
- Describe the results of the assessment
- Identify if there is adverse or a potentially adverse impacts for any equalities groups

There is no impact on equality.

**Conclusion**
- Provide a summary of the overall conclusions

The policies apply to all staff regardless of race, ethnic origin, gender, culture, religion or belief, sexual orientation and age.

**Recommendations**
- State recommended changes to the proposed policy as a result of the impact assessment
- Where it has not been possible to amend the policy, provide the detail of any actions that have been identified
- Describe the plans for reviewing the assessment

The policy should be approved.
APPENDIX 2: CHECKLIST FOR THE REVIEW AND APPROVAL OF DOCUMENTS

To be completed (electronically) and attached to any document which guides practice when submitted to the appropriate committee for approval or ratification.

**Title of the document:** Portable Computer Device Policy  
**Policy (document) Author:** Malcolm Flier, Head of IT  
**Executive Director:** Simon Marshall, Director of Finance and Information

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Yes/No/Unsure/NA</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Title</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the title clear and unambiguous?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is it clear whether the document is a guideline, policy, protocol or standard?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Scope/Purpose</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the target population clear and unambiguous?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the purpose of the document clear?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are the intended outcomes described?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are the statements clear and unambiguous?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Development Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is there evidence of engagement with stakeholders and users?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Who was engaged in a review of the document (list committees/individuals)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Has the policy template been followed (i.e. is the format correct)?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Evidence Base</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the type of evidence to support the document identified explicitly?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are local/organisational supporting documents referenced?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Approval</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Does the document identify which committee/group will approve/ratify it?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If appropriate, have the joint human resources/staff side committee (or equivalent) approved the document?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Dissemination and Implementation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is there an outline/plan to identify how this will be done?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Does the plan include the necessary training/support to ensure compliance?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Process for Monitoring Compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes/No/Unsure/NA</td>
<td>Comments</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Are there measurable standards or KPIs to support monitoring compliance of the document?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Review Date</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the review date identified and is this acceptable?</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Equality Impact Assessment (EIA)</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Has a suitable EIA been completed?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Committee Approval: Information Governance Steering Group**
If the committee is happy to approve this document, please complete the section below, date it and return it to the Policy (document) Owner

<table>
<thead>
<tr>
<th>Name of Chair</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Ratification by Management Executive (if appropriate)**
If the Management Executive is happy to ratify this document, please complete the date of ratification below and advise the Policy (document) Owner

**Date:** n/a