Ashford and St. Peter's Hospitals
NHS Foundation Trust

Portable Computer Device Policy

Author: **Head of IT**

Executive Lead: **Simon Marshall, Director of Finance and Information**

Status: Approval date: Feb 2019

Ratified by: Information Governance Steering Group

Review date: Feb 2022

Patients first • Personal responsibility • Passion for excellence • Pride in our team

History

Issue	Date Issued	Brief Summary of Change	Author
1	Nov 08	Amendments to cover Encryption standards	Director of Planning and Information
2	Nov 09	Amendments to cover non-Trust-owned portable devices	IM&T Strategy Steering Group
3	Sept 10	Amendments to Departmental names. Addition of Monitoring and Review of Policy	Information Governance Steering Group
4	Dec 12	Amendments to Departmental names and titles. Amendment to Anti-Virus provider	
5	Nov 2015	Amendment to signatory definition of Remote Access Form approval Added name of new Encryption software Modified to new format	Interim Head of IT
6	Dec 2018	Updated: Author Updated: Executive summary Updated sections 2 – 6 Updated section 8	Head of IT
7	Jan 2019	Updated section 13	Head of IT

For more information on the status of this document, please contact:	
Policy Author	Head of IT
Department/Directorate	Health Informatics / Finance
Date of issue	Jan 2019
Review due	Jan 2022
Ratified by	Information Governance Steering Group
Audience	All Staff

Executive summary

Ashford and St Peter's Hospitals NHS Foundation Trust (ASPH) has a responsibility to ensure that all data stored on its computer systems is appropriate to the needs of the organisation, is stored securely, is available in a complete and accurate form when needed and complies with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). 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. Personal portable devices are out of scope for the purposes of this policy but are covered in the over-arching Information Security Policy.

For the purpose of this policy, the term "portable device" includes laptops, PDAs, notebooks, tablets (iOS, Android), tablet PCs, hand held devices (e.g. iPod Touch), Mobile Clinical Assistants (MCAs) and mobile Smart phones owned by the Trust.

Contents

Appendices

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 Foundation 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 and covers Trust-owned portable computer devices. Personally-owned devices (e.g. personal Smart phones) are excluded but are covered in the over-arching Information Security Policy.

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, tablets (iOS, Android), tablet PCs, hand held devices (e.g. iPod Touch), Mobile Clinical Assistants (MCAs) and mobile phones owned by the Trust.

4. Explanation of Terms Used

4.1 PDA – Personal Digital Assistant. This is a legacy term for a type of lightweight consumer electronic device that looks like a hand-held personal computer but only performs a limited range of tasks.

4.2 MCA- Mobile Clinical Assistants. This type of device is a handheld PC designed specifically for use in clinical areas. Typically these are more robust and easier to clean than standard PCs.

4.3 RAS - Remote Access Service. This is a web service that allows Trust staff to connect securely to the Trust's corporate network over the internet from any compatible device, including personal devices.

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.

4.7 GDPR – the European General Data Protection Regulation.
4.8 DPA – the Data Protection Act 2018.
4.9 PID – Patient/Person Identifiable Data (name, address, DOB, etc.), which includes staff records
4.10 CPI - Confidential Patient Information (e.g. health record, diagnosis, etc.)

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 DPA, GDPR and the Caldicott Principles.
- Portable device users must take personal responsibility for the security of the equipment, software and data in their care and abide by the following:
- 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 when the car is unattended. The device should be taken indoors overnight wherever possible
- Users must return the portable device to the IT department for regular health checks (see below) or when requested
- Devices must be brought onsite, ideally on a monthly basis to ensure all security and anti-virus definitions are up to date.
- Return the portable device before leaving the employment of the Trust
- Report any possible security breaches (e.g. portable device stolen or misplaced) to the IT Helpdesk / department immediately.
- Avoid saving data to the device by using the Trust's Remote Access Service (RAS) to save data directly to the Trust network. Data stored on the network can be accessed and modified in the same way.
- Where use of the RAS is not possible, the user is responsible for ALL data saved on the device. It is recommended that portable devices are brought in on a regular basis and data copied to the network and then removed from the device.

5.2 Department Owner Responsibilities

Where a portable device is for departmental use and not for the sole use of an individual member of staff a department owner for the portable device must be identified.

- The department owner will be responsible for:
  a. Complying with Trust standards on data encryption, ensuring that any encryption passwords are only issued to authorised staff
  b. Ensuring that the portable device is issued only to authorised staff
  c. Keeping a record of who the portable device is issued to within the department
  d. Returning the portable device to the IT Department for regular health checks and when requested (see above for frequency)
  e. Ensuring staff are aware of the User Responsibilities as detailed above

5.3 IT Department Responsibilities

It is the responsibility of the IT Department to ensure the correct configuration of portable 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 Department will remind staff to bring their devices onsite on a regular basis to log into the network to receive important updates.

6. Policy

The Trust has a responsibility to ensure that all data stored on its computer systems is appropriate to the needs of the organisation, is stored securely, is available in a complete and accurate form when needed and complies with the requirements of the DPA and the GDPR. The use of portable computer devices increases the risks associated with the data storage.

Further guidance on the use of PID and CPI 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, abroad, etc.. This service is available for users with portable devices. A RAS application form (available on TrustNet) must be completed, signed by the user's line manager and approved by the Trust's Head of IT. Users must comply with the RAS agreement as stated on the application form.

Person Identifiable Data (PID) and Confidential Patient Information (CPI)

PID and CPI must be stored in a portable device only when necessary.

Where it is necessary to store such information, the following conditions apply:

- For work involving PID/CPI, users are required, wherever possible, to use the Trust network to store the data.
- Only the minimum amount of PID/CPI necessary for the current purpose, shall be stored.
- PID applies to both patients and staff records, and includes, but is not limited to, the following:
  - NHS Number
  - Forename
  - Surname
  - Date of Birth
  - Sex
  - Address
  - Postcode

CPI includes, but is not limited to, the following:

- Medical Record items, such as letters and forms about the patient's health

- Diagnosis,
- Medications
- PID not be stored on a portable device other than as described previously in this policy
- Password authentication must be applied
- Measures should 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.

Virus Protection

All Windows devices have the Trust approved Anti-Virus software installed at the time they are issued. The anti-virus system **must** be updated on a regular basis as described earlier in this policy. It is the responsibility of the device 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 ASPH Internet Usage and Security Policy applies to Trust portable computer devices, whether used on the hospital network, at home or in any other location.

New and replacement mobile devices

Where a laptop is required to work from home, you must relinquish your PC. This will be replaced with the laptop and a docking station.
If a new mobile hand-held device is required, you must complete the 'Mobile Device Justification' section in the IT Equipment Order Form which can be downloaded from Trustnet.

7. Training

No training is required.

8. Stakeholder Engagement and Communication

The policy has been written by the Health Informatics Team and is reviewed and approved by the Information Governance Steering Group. The policy is available to all staff on TrustNet.

All new staff are 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 authors 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 the Information Content Manager (Quality and Communications Teams) 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

This document will be monitored regularly to ensure it is effective and to assure compliance

Requirement to be monitored	Leads	Tool	Frequency of monitoring	Reporting Arrangements	Lead(s) for acting on recommendations
This policy will be regularly reviewed and updated	IT Department and Information Governance lead(s)	Report to Information Governance Steering Group	At least every 3 years or more frequently if required	HIS policy audit report to: Information Governance Steering Group	Assigned by 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: Morné Beck, Head of IT
Policy: Portable Computer Device Policy

Background • Who was involved in the Equality Impact Assessment
The EIA was performed by the Head of IT
Methodology • 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) • The data sources and any other information used • The consultation that was carried out (who, why and how?)
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 impact 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

		Yes/No/ Unsure/ NA	Comments
1.	**Title**		
	Is the title clear and unambiguous?	**Yes**	
	Is it clear whether the document is a guideline, policy, protocol or standard?	**Yes**	
2.	**Scope/Purpose**		
	Is the target population clear and unambiguous?	**Yes**	
	Is the purpose of the document clear?	**Yes**	
	Are the intended outcomes described?	**Yes**	
	Are the statements clear and unambiguous?	**Yes**	
3.	**Development Process**		
	Is there evidence of engagement with stakeholders and users?	**Yes**	
	Who was engaged in a review of the document (list committees/ individuals)?		
	Has the policy template been followed (i.e. is the format correct)?	**Yes**	
4.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?		
	Are local/organisational supporting documents referenced?		
5.	**Approval**		
	Does the document identify which committee/group will approve/ratify it?	**Yes**	
	If appropriate, have the joint human resources/staff side committee (or equivalent) approved the document?		
6.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	**Yes**	
	Does the plan include the necessary training/support to ensure compliance?		
7.	**Process for Monitoring Compliance**		

		Yes/No/ Unsure/ NA	**Comments**
	Are there measurable standards or KPIs to support monitoring compliance of the document?	**Yes**	
8.	**Review Date**		
	Is the review date identified and is this acceptable?	**Yes**	
9.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?		
10.	**Equality Impact Assessment (EIA)**		
	Has a suitable EIA been completed?	Yes	

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			
Name of Chair		**Date**	
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			