

Master ID

Version

Document Name

Type

Date adopted

Review Date

Responsibility for Review

Equality Impact Assessment Performed

Approved by

Mobile Working and Remote Access Facility Policy

Contents

1. Introduction and Purpose
2. Definitions
3. Accountability and Responsibility
4. Process for monitoring compliance with and effectiveness of the policy/guidelines/procedure
5. References
6. Consultation
7. Process for review of the document

Appendix A: Mobile working approval form

1. Introduction

The use of portable devices and mobile computing equipment is now commonplace in the NHS with users connecting remotely to required information services through laptops, Blackberry's etc. Users are also connecting from a variety of locations – home, hotels, NHS and council premises, and through internet, wireless and dial-in technologies. Mobile computing and teleworking pose a substantial risk in that devices may be lost, damaged, or stolen, potentially resulting in loss or inappropriate disclosure of data. When using mobile computing, the risks of working in an unprotected environment must be considered and mitigated where possible by the use of appropriate security procedures or facilities. It is essential therefore that mobile working and remote access to PCT systems are approved in advance in order that the organisation can be assured that Staff working remotely do so safely and securely.

The Trust's Policy is that remote access to the network will be subject to robust authentication and that VPN connections to the network are only permitted for authorised users ensuring that use is authenticated and data is encrypted during transit across the network.

Equipment holding Trust data is an information asset and must be recorded on the Trust's Information Asset Register

2. Definitions

VPN

A 'virtual private network (VPN) is a computer network that uses a public telecommunication infrastructure such as the Internet to provide remote

offices or individual users secure access to their organization's network. It aims to avoid an expensive system of owned or leased lines that can be used by only one organization.

Encryption

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key

WIFI

A Wi-Fi enabled device such as a personal computer, video game console, smartphone, or digital audio player can connect to the Internet when within range of a wireless network connected to the Internet.

3. General Policy Statements:

Mobile working and remote working must be authorised and controlled by senior managers or directors

The Trust's approved method of remote connection is the virtual private network (VPN) managed by OHIS Services. The user needs to input username and password which ensures strong authentication in line with Department of Health requirements. Access to desktop email, diary and some of the Trusts clinical systems is possible using the VPN.

Users will be required to sign a declaration before VPN access is granted.

Trust owned mobile devices and media must be encrypted if they contain person identifiable information (PID) or other sensitive data. Any sensitive data sent to or from that device should be encrypted during transit.

Mobile phones and similar devices used for email access must have the security PIN number enabled.

In accordance with the NHS Statement of Compliance, only Trust owned or managed equipment is to be connected to the Trust's network. This includes all mobile devices.

Person identifiable data (PID), or other confidential Trust data must not be stored permanently on mobile devices or media .Where possible information should be transferred to the Trust's secure network and deleted from the device as soon as possible.

Unauthorised software must not be installed onto Trust mobile devices

Anti virus scanning software must be installed and regularly updated.

Redundant Trust equipment must be returned to OHIS for secure disposal

4. Accountability and Responsibility

Information Risk Management

The NHS structured approach to information risk management has been implemented within the PCT as follows:

Printed versions of this document may be out of date.

258 Non-Clinical Mobile Working and Remote Access Facility Policy March 2011

- Accountable Officer (AO) Chief Executive
- Senior Information Risk Owner (SIRO) Director of Strategy and Quality
- Information Asset Owners (IAO) Directors and senior/service manager

Directors

Directors are responsible for the management of information risk within their Directorate and in particular are responsible for ensuring their staff are aware of the information risks identified within this policy and take responsible action to mitigate them.

Directors must -

- ensure procedures are in place within their Directorate to enable the identification and assessment of information risks of mobile computing and remote working and the implementation of control measures, including staff training and awareness to mitigate the risks.

- ensure all mobile and teleworkers are appropriately approved and authorised. This should include a procedure to ensure that mobile computing and removable media devices used are approved for Trust equipment that has been encrypted.

- undertake regular audits to ensure: -

- all users are approved

- that all mobile devices issued can be accounted for and

- that assurance can be given to the SIRO that identified

risks are adequately controlled and managed.

All Staff

All staff, whether permanent, temporary or contracted, must be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality and understand they are required to comply with this policy. Failure to comply with this policy may result in disciplinary action being taken, which may result in the withdrawal of authorisation and facility to work remotely.

Staff shall inform their manager if they have any concerns about any issues that would constitute an information risk. This covers not only risks to resources or confidentiality of data, but also personal risk, risk to others and risk to the Trust's reputation.

Staff need to confirm to their line manager that they understand this policy and their responsibility for the protection and security of the Trust information they access. They must agree with their manager how they will comply with this policy when working away from OPCT controlled premises.

Authorisation must be obtained from the individual's line manager before any patient or staff or confidential information is taken away from the normal work location.

Trust information must only be used for Trust related purposes in connection with Trust work.

Staff who are authorised to work remotely, or from home, shall only access the Trust information that they need in order to do their job by either: -

- Remote VPN connection, or

Printed versions of this document may be out of date.

258 Non-Clinical Mobile Working and Remote Access Facility Policy March 2011

Page 3 of 6

- Use of an encrypted mobile device, such as a Blackberry, issued by the Trust

Holding person identifiable data on anything other than Trust equipment is a breach of the Data Protection Act 1998. Staff are not permitted to hold person identifiable data or any other Trust sensitive data on personally owned equipment, in particular home PCs. This includes, for example, uploading Trust data from removable media directly onto the hard drive of a personally owned PC at home, or bypassing the secure encryption methods by emailing confidential or sensitive Trust information to their personal email accounts.

Holding other commercially or business sensitive Trust data on personal equipment would breach Trust policies concerning information security and records management.

Staff who regularly work remotely should access information directly from the Trust's systems via the VPN to avoid having to transport information and to mitigate the risk of accidental loss of data and equipment.

Where the Trust has supplied any form of mobile device or media, only appropriately authorised members of staff are allowed to have any access to it. Staff must not allow an unauthorised person to use and/or access information held on the device, e.g. a member of their household, either deliberately or inadvertently.

Staff must not, under any circumstances, disclose their network user name, or password, or personal PIN number to anyone or allow anyone to use their VPN to gain access to Trust data.

Staff must not connect any Trust supplied equipment to any phone line, internet connection (including WiFi) or other computer, unless they have been given written authority by the Trust's Information Security Advisor and access to either the NHS network or the Trust's network via a secure remote link.

Where staff have been supplied with a mobile device they are responsible for ensuring that it is regularly connected to the Trust's network 'onsite' for upgrade of antivirus software and other licensing requirements.

Staff working remotely by using portable devices or removable media must keep equipment, files and media locked out of sight during transit, and must also ensure any equipment is not left either unattended or insecure when off site to prevent accidental loss and unauthorised access at all times, including within their home. Particular care must be taken when media and equipment are taken on to public transport.

The use of personal information in public areas must be kept to an absolute minimum, due to the threats of 'overlooking' and to discourage theft.

Staff are responsible for ensuring that unauthorised individuals are not able to see any confidential Trust information or access Trust systems. Only

Printed versions of this document may be out of date.

258 Non-Clinical Mobile Working and Remote Access Facility Policy March 2011

Page 4 of 6

members of staff are allowed access to information being used at home in any form, on any media.

Establishing support arrangements for software on non Trust PCs e.g. personal PCs at home, necessary to access Trust data via VPN is the responsibility of the staff member/user. No support is provided by the ICT department or helpdesk.

All users are required to understand and abide by the principles laid down in this policy document. Users must treat Remote Access and Mobile Computing systems as if they were using Trust systems from their desk based onsite.

Staff must ensure that removable media must not be used to store inappropriate images or files, and the content of all information stored on mobile devices and media is in line with Trust policy.

5. Process for monitoring compliance and effectiveness of the policy/guidelines/procedure

Regular audits should be undertaken to ensure all users are approved, that mobile devices issued can be accounted for and that assurance can be given to the SIRO that identified risks are adequately controlled and managed.

Adherence to this policy will be monitored via the investigation and analysis of information security incidents reported to the Information Governance Committee by the Information Security Adviser.

6. References

Information Governance Policy

<http://nww.oxfordshirepct.nhs.uk/PlanningAndSystemReform/Document%20Library/Policies,%20guidelines%20and%20procedures/044%20Non-Clinical%20Information%20Governance%20Policy%20August%202010.pdf>

Home Working Policy and Guidelines

<http://nww.oxfordshirepct.nhs.uk/HumanResources/Document%20Library/Policies,%20Guidelines%20and%20Procedures/226%20Human%20Resources%20Home%20Working%20Policy%20August%202009.pdf>

Information Security Policy

<http://nww.oxfordshirepct.nhs.uk/PlanningAndSystemReform/Document%20Library/Policies,%20guidelines%20and%20procedures/247%20Non-Clinical%20Information%20Security%20Policy%20Sep%202010.pdf>

7. Process for review of the document

The Information Governance Committee is responsible for the review of this policy every 2 years.

Printed versions of this document may be out of date.

258 Non-Clinical Mobile Working and Remote Access Facility Policy March 2011

Page 5 of 6

Appendix A

Mobile Working Authorisation Form

Name:

Staff ID no.

Job Title:

Department/Directorate:

Contact Number:

Trust e-mail account.....

Please detail the work you are undertaking:

I (name) have read and understood and will abide by the terms of the Mobile Working Policy.

I understand that any violation of this policy could result in disciplinary action and possible dismissal or criminal prosecution.

Signed: Date:

Authorisation:

Name:

Job Title:

Contact Number:

Signed: Date: