Mersey Care NHS
NHS Foundation Trust

Policy Number	SS02
Policy Name	Remote Working & Mobile Devices Security Standard
Policy Type	Trust-wide Non-clinical
Accountable Director	Director of informatics and Performance Improvement (SIRO) and Medical Director (Caldicott Guardian)
Author	IM&T Security Manager
Recommending Committee	Joint Senior Information Risk Owner / Caldicott Committee
Approving Committee	Acquisitions Steering Group
Date Originally Approved	December 2015 (Reviewed July 2016)
Next Review Date	December 2017

This document is a valid document, however due to organisation change some references to organisations, organisational structures and roles have now been superseded. The table below provides a list of the terminology used in this document and what it has been replaced with. When reading this document please take account of the terminology changes on this front cover

Terminology used in this Document	New terminology when reading this Document
Mersey Care NHS Trust	Mersey Care NHS Foundation Trust
Executive Director of Finance	Director of Informatics and Performance Improvement
Deputy Chief Executive	Director of Informatics and Performance Improvement
Joint Information Governance and Caldicott Committee Joint Information Governance and Senior information owner committee	Joint Senior Information Risk Officer / Caldicott Committee

Mersey Care NHS
NHS Trust

TRUST-WIDE NON-CLINICAL DOCUMENT

Remote Working & Mobile Devices Security Standard

Standard Number:	**SS02**
Scope of this Document:	**All Staff**
Recommending Committee:	**Joint Information Governance & Caldicot Committee**
Approving Committee:	**Joint Information Governance & Caldicot Committee**
Date Ratified:	**December 2015**
Next Review Date (by):	**December 2017**
Version Number:	**Version 2**
Lead Executive Director:	**Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO) / Medical Director / Cadicott Guardian**
Lead Author(s):	**IM&T Security Manager**

TRUST-WIDE NON-CLINICAL DOCUMENT

2016 – Version 2

Quality, recovery and wellbeing at the heart of everything we do

Mersey Care NHS Trust

TRUST-WIDE NON-CLINICAL DOCUMENT

REMOTE WORKING & MOBILE DEVICES SECURITY STANDARD

Further information about this document:

Document name	**Remote Working & Mobile Devices Security Standard SS02**
Document summary	**Trust Standard on the use of Remote Working & Mobile devices**
Author(s) Contact(s) for further information about this document	**Mark Williams** **IM&T Security Manager** **Telephone: 0151 472 4031** **Mark.Williams@merseycare.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Trust** **Trust Headquarters** **V7 Building** **Kings Business Park** **Prescot** **L34 1PJ** **Your Space Intranet: http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IM&T Security Policy IT02**
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

Version History:		
Draft	Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO) / Medical Director / Cadicott Guardian	December 2015
Version 2	Acquisition Steering Group	June 2016

SUPPORTING STATEMENTS – this document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Trust employees have a statutory duty to safeguard and promote the welfare of children and vulnerable adults, including:

- being alert to the possibility of child/vulnerable adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/vulnerable adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/vulnerable adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or vulnerable adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

Contents

1 PURPOSE AND RATIONALE

1.1 **Purpose** –Current Health and Social Care models of delivery are such that staff may need to access Trust information from a location that is not their normal work base. For example, individuals may not have a static work base or they may occasionally work away from their normal place of work. In addition, flexible working practices mean that some staff may be working from home on a regular or ad-hoc basis.

Developments in technology are such that it is possible to process information using various types of portable (mobile) electronic devices such as laptops, tablet notebooks and USB memory sticks, enabling staff to work at different locations and while they are 'on the move'. While these developments bring many benefits, they also introduce risk to the organisation and individual staff members relating to the security of Trust information. The convenience of these devices, their small size and capacity to hold large amounts of information, presents their greatest risk as they can easily be lost, mislaid or stolen. Therefore, it is critical that Trust information, whether held on mobile devices or accessed remotely, is protected by appropriate security.

1.2 **Rationale** –This Remote Working and Mobile Devices Security Standard is to protect Trust information that is processed remotely or is stored on portable devices. It forms part of the Trust policies and should be read in conjunction with the IM & T Security Policy.

2 OUTCOME FOCUSED AIMS AND OBJECTIVES

2.1 *For this Security Standard the aims and objectives are as follows:*

(a) To ensure the use of mobile devices on behalf of the Trust is carried out safely and securley, safeguarding the security and confidentiality of the data held on these devices.

(b) To ensure that the Trust's staff fully understand the correct methods of Remotley connecting to the Trust's Infrastructure to maintain security.

(c) To ensure staff understand their responsibilities when using mobile devices and remote virtual private networking.

(d) To highlight potential risks associated with using mobile devices and working remotely.

(e) To ensure staff know what to do and who to contact if a mobile device is lost or stolen.

3 SCOPE

3.1 Remote working (working on Trust information or accessing the Trust network in a place that is not your normal work base or work station)

3.2 The use of portable processing devices (laptops and notebooks, iPads and other tablets, smart phones, such as Blackberries and personal digital assistants (PDAs), digital cameras, other mobile phones and any other mobile devices which process information)

In particular, the standard covers:

a) Connection to the Trust network remotely and with portable devices

b) The processing of Trust information away from Trust premises

c) The processing of Trust information on portable devices

d) The secure transfer of information

e) The security of portable devices and information

3.3 This Standard applies to all users of Trust systems and equipment, including Trust employees and non-Trust employees who work within Mersey Care NHS Trust, or under contract to it. This includes, but is not limited to, staff on secondment to the Trust, students on placement and those working in a voluntary capacity.

3.4 The term 'staff' is used in this document to refer to all those to whom the Standard applies.

3.5 This Standard is based on current law, NHS Information Governance standards and accepted standards of good practice; your duty to handle Trust and person identifiable information appropriately arises out of common law, legal obligations, staff employment contracts and professional obligations.

3.6 This standard governs all staff who have access to Trust information, that is, all staff who work at the Trust and not only those who have access to the Trust network.

3.7 Any breaches of this Standard may result in your employment or your association with the Trust being terminated. It may also bring into question your professional registration and may result in disciplinary, civil or criminal proceedings.

3.8 If there is anything that is not clear or which you do not understand in this document you must contact your Line Manager, in the first instance, or the Information Governance Manager or IM&T Security Manager for further information/ clarification**.**

Please note the procedures and policies outlined in this Standard and any related Standard may be changed at any time. You will be alerted to this via established Trust communication routes such as team brief, weekly and monthly round up, intranet and internet.

4 RESPONSIBILITIES

4.1 All managers are responsible for ensuring the staff they manage are aware of the IM & T Security policy and their individual responsibility for compliance. They should ensure their staff are equipped to fulfil those responsibilities; this will include covering

this subject in local induction and by identifying and meeting specific and generic training needs through the PDR process.

4.2 Managers are required to ensure staff have read and understood the IM & T Security policy and this Standard and have had an opportunity to ask questions about anything that requires clarification.

4.3 Senior managers should ensure that managers within their Service are aware of their responsibilities in relation to informing staff about acceptable standards of information governance.

4.4 All staff must ensure that they are aware of the requirements and standards of behaviour that apply.

4.5 All staff are responsible for reporting information incidents and near misses, including breaches of this standard using the Trusts incident reporting mechanism. Access to this can be found on the Trust web site and further information can be obtained from the IM&T Security Manager or Information Governance Manager.

4.6 The Trust Joint Information Governance and Senior Information Risk Owner Committee is responsible for overseeing the implementation and monitoring compliance of this Standard. It is responsible for ensuring it is reviewed periodically.

5 NETWORK CONNECTION

5.1 Direct Connection -All electronic processing devices connecting directly to the Trust network (that is, connected to a network point or wireless access point on Mersey Care premises) must be protected by up-to-date anti-virus software. Where the device does not update its software automatically it is the responsibility of the user to ensure that the anti-virus software is up-to-date.

5.2 Personal devices - (devices that are not provided by your employer) such as home personal computers, laptops and media players such as iPads, must not be connected directly to the Trust network.

5.3 Remote Access -The Trust recognises that from time to time Trust staff will need to work from home or other remote locations. The Trust has implemented a VPN (Virtual Private Network) solution to enable staff to work remotely and securely from home and other non-NHS locations. This policy and the procedures in it apply to your use of the Trust*'s* systems and to your use of Trust laptops and your own computer equipment when you are working on Trust*'s* business away from the Trust*'s* premises (working remotely).

5.4 When you are working remotely from home or a non-NHS site you must: not install VPN clients on any computer. Only Informatics Merseyside can install VPN and set up remote access. The VPN client can only be installed on Trust owned or approved computers;

5.5 Password protect any work which relates to the Trust*'s* business so that no other persons can access your work and keep the password secret;

5.6 Position yourself so that your work cannot be overlooked by any other persons. Take reasonable precautions to safeguard the security of our laptop computers, any computer equipment on which you do the Trust's business and your passwords;

5.7 Apply an appropriate level of security to any personal data which comes into your knowledge, possession or control through your employment with the Trust so that the personal data is protected from theft, loss, destruction or damage and unauthorised access and use;

5.8 If a device is lost or stolen the Service Desk must be informed immediately and the user must contact police who will supply an incident number.

5.9 When working remotely from an NHS site you are permitted to access Mersey Care systems from NHS PCs via encrypted Terminal Server Connections.

5.10 Third Party Remote Access –Where there is a requirement for third parties to access the network for remote support, this needs to be requested via the Service Desk.

5.11 The Trust has implemented a VPN Solution (Virtual Private Networks) to enable third party support. This technology uses a token-based access control providing two factor authentication.

5.12 The third party secure tokens must be stored by Informatics Merseyside. Only Service Desk support has access to the secure tokens.

5.13 All access to the Trust's network is logged for audit purposes.

5.14 The Trust does supply free access to its wireless network but the traffic is routed away from all Trust resources and data stores.

6 PORTABLE DEVICES

6.1 Only encrypted laptops and USB sticks that have been provided/ authorised for use by Informatics Merseyside may be used. The use of personal USB memory sticks is not permitted on Trust equipment with the exception of the USB devices provided in learning and development provided by the local ICT service desk at Calderstones division.

6.2 All Trust iPads/ Android devices must be centrally managed by Airwatch (the Trust Mobile Device Management solution). Use of these devices requires users to undertake security training and to accept the terms and conditions of acceptable use prior to issue. For more information please contact the Service desk or the IM&T Security Manager.

6.3 The procurement of portable media / mobile devices must be authorised by the IT Department. It is the responsibility of the line manager to ensure that any equipment purchased for mobile working or mobile devices are returned when a member of staff leaves the employment of the Trust and the updated records are passed to Informatics Merseyside as to who the equipment has been reallocated to.

6.4 The use of portable media must be authorised by your Line Manager or Information Governance/ IT Services, where appropriate.

6.5 Portable devices can be used to transport information or to enable information to be worked on remotely. However, all information, whether confidential or otherwise, is only to be transferred using encrypted portable media and should only be used to transport confidential or sensitive information when other more secure methods are not available.

6.6 Portable media is a means for transferring data. It is not intended to be a long-term storage medium nor is it an adequate back up device. The Trust's network provides all users with the facilities to save information securely in shared folders that are backed up on a daily basis.

6.7 Always transfer documents back to their normal storage area as soon as possible. Failure to do this may result in problems with the version control or the loss of information if the portable device is lost or corrupted.

6.8 Always remove information from portable media after it is no longer needed. For further advice please contact the Service Desk

6.9 In the event of loss, theft or damage to your portable device, you should contact the IT Service Desk as soon as possible. You must ensure that any suspected or actual breaches of security are reported to the Information Governance Officer directly or via the Service Desk.

6.10 Trust portable devices - Confidential Trust information may only be held on Trust portable devices with the approval from the Joint Information Governance and Senior Information Risk Owner Committee.

6.11 Information must not be stored permanently on portable devices. If it is necessary to use a portable device to process information; the information should be transferred to the Trust server at the earliest opportunity and then deleted from the device.

6.12 Unauthorised software must not be installed onto Trust portable devices.

6.13 Personal portable devices -Trust information must not be stored on non-Trust equipment, for example, home personal computers, laptops, PDAs and mobile phones unless it is part of an agreed process authorised by the Trust Joint Information Governance and Senior Information Risk Owner Committee.

6.14 External visitors such as lecturers, contractors, company representatives, patients or their representatives etc. must not connect any device, including USB sticks and laptops, or insert any media to any equipment belonging to the Trust. Unencrypted USB sticks will be accessible as read only.

6.15 All Trust mobile devices need to be returned to the IT Department periodically for patches and updates and must be made available for inspection upon request.

7 PASSWORDS

7.1 Passwords or passphrases must not be written down and kept with the portable device or in an obvious place in an identifiable manner, for example, in your diary under 'laptop password'. However, it is acceptable to set a password hint to help you to remember your password/ passphrase but ensure this is not too obvious.

If you suspect someone may know your password you should change it immediately. If the device is a pool device, you should inform the pool manager.

The Service Desk can reset passwords

8 SECURITY OF INFORMATION ON PORTABLE DEVICES

8.1 Confidential information, whether manual or electronic, and portable devices must be protected by adequate security and must be:

a) Kept out of sight in the locked boot of the car when being transported.
b) Not left unattended in the car boot overnight or when away from the vehicle.
c) Locked away when not being used.
d) Kept secure and guarded from theft, unauthorised access and adverse environmental events particularly when taken home.

9 FURTHER INFORMATION

9.1 Further information can be obtained from the Trust Information Governance Manager or the IM&T Security Manager.

9.2 Questions about the use of portable devices or any problems in accessing the Trust system should be directed to the IT Service Desk.