NHS
North Yorkshire and York

Title:	**Mobile Computing Procedures**
Reference No:	NHSNYY/003
Owner:	Director of Finance and Contracting
Author:	AD of Informatics
First Issued On:	February 2011
Latest Issue Date:	June 2012
Operational Date:	February 2011
Review Date:	April 2013
Consultation Process:	List stakeholder groups etc consulted
Policy Sponsor:	Director of Finance and Contracting
Ratified and Approved by:	Information Governance Steering Group
Distribution:	All staff
Compliance:	Mandatory for all permanent & temporary employees, contractors, sub-contractors of and those who work jointly with North Yorkshire and York PCT
Equality & Diversity Statement	This policy has been subject to a full equality & diversity impact assessment

CHANGE RECORD			
DATE	AUTHOR	NATURE OF CHANGE	VERSION No
Nov 2010	AD Informatics	First Draft	0.001
Jan 2011	AD Informatics	Amendments following consultations	0.002
Feb 2011	AD Informatics	Final minor changes	1
Feb 2012	IT Services Manager / IT Project Manager	Minor changes	1.1

June 2012	AD Informatics	3.1.1 be changed to read: 'Due to the inherent security risks, once the mobile equipment has been connected to a non-PCT network (i.e. broadband or other internet connected network) it cannot be reconnected directly onto the PCT network unless connecting to an NHS organisational wireless or wired network access controlled area'.	1.2

CONTENTS

1 INTRODUCTION

1.1 Scope:

1.1.1 The guidance and standards outlined below are designed to ensure that the information and equipment belonging to NHS North Yorkshire and York used outside the office environment is afforded similar levels of protection as that equipment and information used exclusively within an office environment. This also extends to information processed within a member of staff's home.

1.1.2 For the purpose of this procedure, the collective name for tablets, laptops, PDA's, blackberries and palmtop computers is 'Mobile IT equipment'. This list is not exhaustive.

1.1.3 This procedure should be read in conjunction with the Use of Encryption Technology Policy.

1.2 Definitions

1.2.1 Laptop is a small, portable computer, small enough that it can sit on your lap. Today, laptop computers are also frequently called notebook computers, though technically laptops are somewhat larger in size than notebooks.

1.2.2 Tablet PC, a type of notebook computer that has an LCD screen on which the user can write using a special-purpose pen, or stylus. The handwriting is digitised and can be converted to standard text through handwriting recognition, or it can remain as handwritten text. The stylus also can be used to type on a pen-based key layout where the lettered keys are arranged differently than a QWERTY keyboard. Tablet PCs also typically have a keyboard and/or a mouse for input.

1.2.3 Encryption renders the contents of a message or file unintelligible to anyone not authorised to read it. It is the conversion of data into a form, called a ciphertext. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

1.2.4 Blackberries are hand-held Smartphone devices. They make use of mobile phone technology to allow users to dynamically receive e-mails, update calendars and surf the web while out of the office and on-the-go.

1.3 General Points

- Users must take due care of mobile IT equipment to prevent accidental damage, e.g. from rough handling or accidentally spilling drinks

- Users must not install any software on mobile IT equipment without prior authorisation from the IT service desk

- As it is accessible from any internet connection, the use of any other personal e-mail accounts (such as hotmail etc) is not authorised for work purposes

- The IT Service Desk will not visit a member of staff's home to fix faulty NHS NYY issued equipment. Following a call to the IT services desk, any mobile IT equipment requiring repair should be delivered to one of the HQ buildings.

- Users who tamper with the hardware and software configuration on mobile IT equipment may have the equipment withdrawn.

- Users must not disable any element of the standard laptop or tablet configuration including data encryption, screen-saver password and anti-virus software

- Valuable information should be backed up to either a network drive or encrypted removable storage media and kept in a separate but secure location, away from the laptop or tablet. If you need advice in backing up information please contact the IT service desk for advice.

- If a member of staff no longer needs to use the Mobile IT equipment due to changes in work processes for example, the mobile IT equipment must be returned to the line manager as specified in section 7.

- All PCT IT facilities, including mobile IT equipment, are provided to help staff perform their role effectively. The use of these facilities for private purposes is generally not permitted, although for Internet and email use please refer to E-*mail and internet Policy.*

- Please read the *Use of Encryption Technology Policy* for more detail on the acceptable use of Mobile IT equipment.

- All users must complete the Connecting for Health Information Security Guidelines Training module and all CBLS and Statutory & Mandatory Information Governance Training before mobile equipment will be issued.

2 MOBILE COMPUTING

2.1 Physical Security

2.1.1 It is important to take all reasonable steps to ensure that any mobile IT equipment is not lost or stolen. This should include leaving it out of sight when away from the workplace, particularly when travelling in a car when it must be locked in the boot.

2.1.2 Mobile IT equipment must not be left in a parked car. At night the mobile IT equipment should be secured in a safe place in the home.

2.1.3 In busy areas such as railway stations, mobile IT equipment should not be placed on the ground, beside you on a counter or left unattended at any time.

2.1.4 All mobile IT equipment must be asset tagged and security marked by the IT Service desk before use.

2.1.5 Care should be taken to ensure safe transport and storage when moving mobile IT equipment between home or other remote locations, and work.

2.2 Software security

2.2.1 All mobile IT equipment will have encryption software installed to ensure security of the information stored on it.

2.2.2 Anti-virus software will be installed on laptops and tablets. This software will be updated when the device is linked to the internet. Apple devices are secured without the use of Anti Virus software.

2.2.3 Mobile IT equipment cannot be guaranteed to provide safe storage of information. In the event that the device is damaged, destroyed or both the main and backup batteries fail, it must be accepted that the information stored on the device will be lost.

2.2.4 The IT Security Officer reserves the right to audit correct usage at any time, and the individual may be held liable for illegally held software or material (e.g. in breach of copyright legislation). The mobile IT equipment could be recalled for these audit purposes.

3 REMOTE ACCESS

3.1 Remote Access Service (RAS)

3.1.1 The PCT currently provides a Remote Access Service (RAS) to allow remote users access to the PCT network. This service enables access for PCT mobile IT equipment that is not directly connected to the PCT computer network. The RAS connection is made through broadband or other internet connected network. Due to the inherent security risks, once the mobile equipment has been connected to a non-PCT network (i.e. broadband or other internet connected network) it cannot be reconnected directly onto the PCT network unless connecting to an NHS organisational wireless or wired network access controlled area.

3.1.2 Access to the PCT network via RAS will only be granted for staff using a secure access token. This method must be used for each RAS session made. A secure access token is a small, calculator-like device that is activated via a PIN number only known to the user. Once activated, the token produces a pseudo random number that is then

used to logon to the RAS system as a one-off password. For every new RAS session this number will be different.

3.1.3 To acquire a secure access token please complete a 'Secure Access Token Request Form' (attached as Appendix C). A secure access token will only be issued to named individuals and only with the knowledge and approval of the individual's service manager.

3.1.4 Once a token has been issued to an individual, they will remain responsible for that token and accountable for any use made of that token with regard to accessing the RAS system. If a token is no longer required it must be returned to the IT Service desk.

3.1.5 The PIN number used to activate the secure access token should only be known to the individual using the token and should not be divulged to anyone. Under no circumstances should the PIN number be written down or stored with the secure access token, as this would constitute a potentially serious security breach. If the user suspects that the PIN number may be known by anyone else they should change the PIN number immediately and notify the IT service desk of potential breach. In addition a PCT incident form should be completed.

3.1.6 If a secure access token is lost or stolen it must be reported immediately to the IT Service desk and a PCT incident form should be completed.

3.1.7 It is the responsibility of the token holder's line manager to ensure that if a member of staff leaves their post or they no longer require their secure access token for any reason, the secure access token is returned to the IT Service desk. If a new member of staff replaces a member of staff in a post, the access token for the outgoing staff must still be returned to the IT Service desk and a new request for a secure access token made for the incoming staff member.

3.1.8 All connections made to the PCT network via Remote Access will be logged. These logs may be subject to auditing from time to time.

3.1.9 When using remote access the user should always be aware that they are potentially connecting to the entire PCT network. They should therefore exercise as much care as if they were using a PC within the PCT. The user should be mindful of any security or confidentiality issues, for example be aware of who else can view the screen while they are using the PC and never leave the PC logged on and unattended, even in the user's own home.

3.1.10 The IT Service Desk will not visit a member of staff's home or work on a PC owned by a member of staff.

4 HOMEWORKING

4.1.1 This will be completed when HR policy is available.

5 LOSS OF EQUIPMENT

5.1.1 Staff should take due care of the Mobile IT equipment and take all reasonable precautions to ensure that it is not damaged, lost or stolen. In the event that the Mobile IT equipment is stolen, staff will be expected to report the theft to the police and obtain an incident number. In addition to this they should also inform their manager, who must inform the IT Security Officer and IT Service Desk and complete a PCT incident form.

5.1.2 If any mobile IT equipment is lost, stolen or damaged, a report must be completed as shown at Appendix A, and returned to the Director of Finance. The reason for this is that the PCT has a duty to keep a losses and compensation register and to report the loss to PCT Board.

5.1.3 All incidents relating to the security of the mobile IT equipment should be reported using the PCT's Incident Reporting procedures. This shall include but is not limited to:-

- Suspected unauthorised use of RAS token
- Theft / loss of portable device
- Disclosure of data to an unauthorised person
- Loss / corruption of data

6 REMOVABLE STORAGE MEDIA

6.1 Universal Serial Bus (USB) memory sticks are very useful devices for moving information between PCs. Only encrypted USB devices issued by the PCT are authorised for use on PCT equipment and to store PCT information.

6.2 As with all technological advances, The IT team welcome and support the use of these devices to save time and improve efficiency, as they can be useful for moving large PowerPoint presentation files quickly and easily from a PC to a laptop.

6.3 However, the proliferation of these devices is not without its problems. Many organisations have found that valuable or sensitive information has inadvertently (or even deliberately) leaked out as a result of the use of these devices. USB Memory Sticks can also be responsible for introducing unwanted files to an organisation such as viruses and unauthorised programs.

6.4 The loss of a memory stick containing or potentially containing sensitive data must be immediately reported to the IT Service desk and a PCT incident report form should be completed.

6.5 Please read the *Use of Encryption Technology Policy* for more detail on the acceptable use of removable storage media.

6.6 USB memory sticks should only be used on the corporate network. Use across outside of the corporate network is not permitted.

7 STAFF LEAVING THE ORGANISATION

7.1 Staff leaving the organisation must return their mobile IT equipment to their Service Manager.

7.2 Secure Access Tokens must also be returned to the Service Manager.

7.3 Service managers will be responsible for making sure that this has been done as part of the normal handing back of organisation property.

7.4 The Service Manager should hand the equipment back to the IT Service desk to be re-configured or put back into stock.

7.5 The Service Manager must work in accordance with the Acceptable Use Guidelines to ensure network access is terminated.

8 INTERNET CONNECTIVITY AND USAGE

8.1 Any portable device (eg blackberry) owned by the organisation, which has Internet connectivity, must be used in accordance with the PCT's E-mail and Internet Policy.

9 WIRELESS AND OTHER CORDLESS CONNECTIVITY

9.1 Technological developments in the area of cordless connectivity (eg Wireless protocols, Bluetooth and Infrared) have significantly increased the risks of unauthorised interception of a signal and of unauthenticated links being made to other devices.

9.2 Staff must not use such connectivity unless encrypted or approved and configured by the IT Service desk. The IT team reserves the right to disable these facilities if deemed necessary.

9.3 Devices which have been connected to any foreign network or Internet Service Provider must not be reconnected to the corporate network.

10 USE OF NON-NHS PURCHASED EQUIPMENT, SOFTWARE AND DATA

10.1 Non-NHS purchased equipment, software and data must never be attached to, or used / loaded onto the PCT network. This includes but is not restricted to PDA's, mobile phones, memory sticks, MP3 players, CDs and DVD's.

10.2 The IM&T Department has no control over the files stored on non-NHS purchased equipment and regards those devices as a potential risk that may introduce viruses and spyware onto the network.

10.3 The PCT has an obligation under the Information Governance Statement of Compliance to ensure that only approved / authorised equipment is connected to the network.

10.4 Any non-NHS purchased equipment found connected to the PCT network will be removed immediately.

11 Implementation and Compliance

11.1 Responsibilities of all Staff

11.1.1 All staff are obliged to adhere to this procedure. It is the responsibility of the individual to ensure that they understand this policy. Managers at all levels are responsible for ensuring that the staff for whom they are responsible are aware of and adhere to this procedure. They are also responsible for ensuring staff are updated in regard to any changes in this procedure.

11.1.2 All staff using Mobile equipment, including personally owned devices should sign the 'Portable Equipment Receipt form' attached at Appendix B, and return to the IT service desk.

11.2 Reference Documents

11.2.1 Use of Encryption Technology Policy.

11.2.2 Email and Internet Policy

11.2.3 Acceptable use Guidelines

11.2.4 Copies of all the above can be found on the PCT's Intranet site

11.3 Distribution

11.3.1 This Procedure will be available on the PCT Intranet.

11.4 Review

11.4.1 This Procedure will be reviewed annually or as requirements change.

North Yorkshire and York

Appendix A

STOLEN, LOST OR DAMAGED PROPERTY REPORT

Date of Incident: .....

If stolen date reported to Police: ..... Incident No .....

Reported to Manager : ..... Date .....

Description of property:

Where stolen from or how damaged:
(If stolen from a vehicle state where stored)

Signed ..... Date .....

Management Action

Action taken:

Signed ..... Date .....

Designation ..... Date …….....

Passed to Finance for Write off .....

Finance Action

Included on Write off statement

Date ……..... ……

Value £

North Yorkshire and York

Appendix B

MOBILE COMPUTING EQUIPMENT RECEIPT FORM

I confirm that I have received Mobile IT equipment and have read, understood and will comply with the Mobile Computing Procedure and all relevant Information Governance policies, as available via the intranet.

Name…….

Base……

Job Title: …….

Manager……..

Employing organisation …….

Signature……..

Date……

For IT Purposes Only:

IT Service Desk Reference Number……

Make and Model: ……...

Type of Mobile IT equipment (eg Laptop)……..

Serial Number……Asset Register Number …… ……

Additional Software Installed……

……..

Additional Hardware……..

IT Technician…… …Signature ……..

Please send the completed form to NHS NYY IT service desk, 1st Floor, Station Road Business Park, Station Road, Thirsk Y07 1PZ or email to ITservicedesk@nyypct.nhs.uk

North Yorkshire and York

Appendix C

NORTH YORKSHIRE AND YORK PRIMARY CARE TRUST

Secure Access Token Request Form

To be completed by the employee's Supervisor/Line Manager.

Date: ……..

User's Details:

User's Full Name: ……

PC Username: ……

Job Title: ……

Department: ……

Supervisor/Line Manager:

Name: ……

Job Title: ……

Department: ……

Signature: ……..

Contact Telephone Number: ……..

Please send the completed form to NHS NYY IT service desk, 1st Floor, Station Road Business Park, Station Road, Thirsk Y07 1PZ or email to ITservicedesk@nyypct.nhs.uk. Either the service manager's signature is required or the form should be e-mailed by the service manager.