Policy Reference – POL011

Wirral Clinical Commissioning Group

LAPTOP AND PORTABLE DEVICES AND REMOTE ACCESS POLICY

Version	**1.0**
Ratified By	**Governing Board**
Date Ratified	**5th March 2013**
Author(s)	**Ian Hart, Chief Operating Officer, Cheshire ICT Service**
Responsible Committee / Officers	**CCG Committee which includes Information Governance in the Terms of Reference**
Issue Date	**5th March 2013**
Review Date	**12 months from date of issue**
Intended Audience	**All CCG Employees**
Impact Assessed	**Yes**

Policy Reference – POL011

This policy covers the following organisations:

- NHS Wirral Clinical Commissioning Group
- NHS West Cheshire Clinical Commissioning Group
- NHS Eastern Cheshire Clinical Commissioning Group
- NHS Warrington Clinical Commissioning Group
- NHS Vale Royal Clinical Commissioning Group
- NHS South Cheshire Clinical Commissioning Group

Policy Reference – POL011

Further information about this document:

Document name	**ICT Service Laptop and Portable Devices and Remote Access Policy**
Category of Document in The Policy Schedule	Corporate
Author(s) Contact(s) for further information about this document	Ian Hart, Chief Operating Officer, **Mark Bakewell** **Chief Finance Officer**
This document should be read in conjunction with	All other ICT Service policies
Published by	**NHS Wirral Clinical Commissioning Group supported by Cheshire ICT Service** **Clark House** **Hurdesfield Industrial Estate** **Hulley Road** **Macclesfield** **SK10 2LU**
Copies of this document are available from	Website: www.wirralccg.nhs.uk/About%20Us/ourpolicies.htm or NHS Wirral Clinical Commissioning Group, Old Market House, Hamilton Street, Birkenhead, Wirral, CH41 5AL

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0		

Table of Contents

1 PURPOSE

To ensure the physical and data security of portable devices owned by Clinical Commissioning Groups (CCGs) and managed and supported by the Cheshire ICT Service.

For the purpose of this policy portable devices can be defined as any equipment upon which Health Service data is held / transported.

At the date of the policy this definition would include portable devices, pen drives, Personal Data Assistants (PDAs) and mobile phones in addition to laptop and tablet Personal Computers (PCs).

2 SCOPE

This policy describes the management and use of portable devices provided by CCGs.

3 HARDWARE AND SOFTWARE

Cheshire ICT Service provides hardware and software which is compatible with CCG systems.

All appropriate hardware and software is procured and installed by the Cheshire ICT Service Delivery and users must not install additional hardware or software.

Staff with non-Cheshire ICT Service provided portable devices are not allowed to connect them to the CCG data Network.

Software downloaded from the Internet must not be loaded onto systems managed and supported by the Cheshire ICT Service.

Software obtained illegally must not be loaded onto the portable device.

Upon termination of employment or contract, the user is required to return all CCG properties as soon as possible, and no later than the last day of their employment/ contractual employment.

The user will exercise care in using and housing CCG equipment.

The Cheshire ICT Service may recall any portable device at any time to audit its use.

4 REMOTE ACCESS

Remote access enables users to gain access to the CCG data network and other work related services. Remote access must be authenticated using an approved authentication method via a VPN token.

Only devices provided by Cheshire ICT Service will be authorised for use.

In order to be considered for remote access to the CCG data network and other work related services, approval must be given from your line manager and the Chief Operating Officer of the CCG, using the form in Appendix A. The remote access application will be managed by Cheshire ICT Service.

5 ENCRYPTED MEMORY STICKS

Allocation of Encrypted Memory Sticks

The allocation of an encrypted memory stick needs to be supported by:

- The budget manager against whose budget the charges will be made.
- The Manager of the service concerned.

Criteria to be met for the allocation of a Cheshire ICT Service approved encrypted memory stick

Two of the following criteria must be met for an encrypted memory stick to be allocated:

- The individual is on official business.
- The individual's post requires them to work off site.
- There is a demonstrable requirement that usage is not likely to be of an ad-hoc nature.
- When the CCG determines that the allocation of a device is needed for business continuity reasons.
- The member of staff is working in a 'flexible' capacity to complete their duties, and the risk of not meeting deadlines can be mitigated to an acceptable level through the availability of a device.
- At the discretion of the Chief Operating Officer of the CCG
- All applications for the allocation of a device must be submitted in writing by the appropriate Manager, Head of Service or Director to the Cheshire ICT Service using the attached pro-forma (see Appendix B). The application must outline the appropriate reason for the request. The budget holder must also approve the application.

On receipt of an encrypted memory stick, the individual will be asked to sign an agreement form (see Appendix C) acknowledging receipt of the device and agreeing to abide by the instructions laid out in the Policy, or be liable for disciplinary action should the user fail to do so.

Where a Cheshire ICT Service approved encrypted memory stick is allocated to a member of staff who is on long-term sick leave or some other prolonged absence from their duties, the manager responsible for that member of staff must consider re-allocating the device to make best use of resources and must notify the Cheshire ICT Service of the temporary transfer.

Where a manager suspects or believes that a Cheshire ICT Service approved encrypted memory stick is being misused, the manager responsible for that member of staff must consider withdrawing the device from the member of staff, pending an investigation to determine the facts.

Staff who are allocated a Cheshire ICT Service approved encrypted memory stick are responsible for:

- Ensuring that the Laptop and Portable Devices and Remote Access Policy is read and understood.
- Ensuring that the device is used in accordance with the Policy.
- Ensuring that if work is being carried out in public places, meeting rooms and other unprotected areas, care is taken to avoid the unauthorised access to or disclosure of the information stored and processed by the portable device.
- Ensuring that the device is kept safe and secure at all times.

6 PROTECTION OF HARDWARE

The user is responsible for safeguarding of the portable device hardware. In this case, it means:

- When not in use, portable devices should be kept in a locked drawer.
- While in transit, portable devices should be in a suitable carrying case and should be kept out of view wherever possible.
- Portable device security is **your** responsibility at all times.
- Do **not** leave the portable device unattended in a public place e.g. car park.
- Do **not** keep password details in the same location as the portable device.
- Avoid leaving the portable device within sight of ground floor windows or within easy access of external doors.

7 SECURITY OF DATA

Confidential data must only be installed on portable devices which have been supplied by the Cheshire ICT Service and have an appropriate level of access security/encryption implemented.

All portable media devices that connect to the CCG data network must be encrypted. Any devices that do not meet this criteria will be blocked from use.

If work is being carried out in public places, meeting rooms and other unprotected areas care should be taken to avoid the unauthorised access to or disclosure of the information stored and processed by the portable device.

Care should be taken by the staff using the portable device to minimise the risk of unauthorised persons overlooking the screen.

Confidentiality Policies apply equally to information whether in the office or at home. Failure to maintain confidentiality may result in a disciplinary action.

A storage solution is provided centrally on the CCG data network and not on each portable device and it is the responsibility of users to utilise this.

The use of the portable device and the data on it must not be shared with family members.

8 VIRUS CONTROL

The portable device has an Anti-Virus software package installed by the Cheshire ICT Service.

This package is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files on the portable device.

CCG users must not alter the configuration of this package.

The anti-virus system's database of virus definitions **must** be updated on a regular basis, each day if possible. This means connecting the portable device to the network for the virus updates to be applied.

9 PASSWORD SECURITY

The CCG Account and Password Management Policy applies in all cases.

10 INTERNET/E-MAIL

The Internet, Email, Network and File Server Policies of the CCG are equally applicable to portable devices.

11 LOSSES AND CONFIDENTIALITY/SECURITY BREACHES

Where there is a potential for breach in patient/staff confidentiality, Reporting the loss / theft of a device to the Risk Manager on DATIX and informing the appropriate person(s) in their department as soon as possible.

Any incident should also be reported to the Cheshire ICT Service Desk.

12 ACCOUNTING/AUDIT

The software and information held on portable devices are subject to the same audit procedures as any other CCG systems.

13 LEGISLATION

Users of portable devices must comply with current legislation regarding the use and retention of patient information and use of computer systems. These include, but are not limited to:

- The Data Protection Act 1998
- Access to Health Records Act 1990
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Freedom of Information Act 2000

14 REVIEW

This policy will be reviewed 24 months from its date of approval. Earlier review may be required in response to exceptional circumstances or relevant changes in legislation.

15 APPENDICES

Appendix A – Remote Access Form

Appendix B - Request Form for Mobile Devices: Encrypted Memory Sticks

Appendix C – Agreement Form: Encrypted Memory Sticks

APPENDIX A

Remote Access Assessment Form

Name of Staff Member	Job Title	Department / Directorate

Statement of Requirements:		

Questions to assist ICT assessment	Y/N	Details
Are you a lone worker?		
What proportion of time do you spend away from your base?		
Do you require access to email and or corporate information outside core hours?		
Are you a member of the CCG Emergency Planning Team?		
Do you have home broadband access?		
Do you have home dial-up access?		

ICT Recommended Solution

Laptop	VPN Token	3G	Blackberry	NHS Mail	Mobile Telephone

Head of ICT Service Development	Signature	Date

Authorisation – Yes / No

Name of Responsible Officer	Signature	Date

APPENDIX B

Request Form for Mobile Devices: Encrypted Memory Sticks

Device required and to be used by:	
Name	Position
CCG	Directorate
Email address	Telephone
Reason for requirement:	
List any other personnel who are likely to use the device: (e.g. names and designations if this is intended as a team device)	
Financial information to cover costs:	
Budget Code	Subjective Code
Name of Budget Manager	Position
Signature	Date

Authorisation:	
Name of Manager /Head of Service / Director	Position
Signature	Date

Completed forms should be returned to:

Cheshire ICT Service
1829 Building
Countess of Chester Health Park
Liverpool Road
Chester, CH2 1HJ

APPENDIX C

AGREEMENT FORM - Mobile Devices: Encrypted Memory Sticks

I agree to abide by the CCG 'Laptop and Portable Devices and Remote Access Policy', which is published on the CCG Website for information.

I agree to return the device when it is no longer needed for official CCG business.

I understand that I may be liable to disciplinary action should I fail to comply with the Policy.

Name	**Position**
Directorate	**Department**
Email address	**Telephone**
Signature	**Date**

Completed forms should be returned to:

Cheshire ICT Service
1829 Building
Countess of Chester Health Park
Liverpool Road
Chester, CH2 1HJ