NHS
North East Hampshire and Farnham
Clinical Commissioning Group

Remote Working and Portable Devices Policy

Subject and version number of document:	Remote Working and Portable Devices Policy. V2.0
Serial Number:	
Operative date:	November 2015
Author:	Information Governance Team, NHS North East Hampshire and Farnham Clinical Commissioning Group
Review date:	November 2017
For action by:	All staff.
Policy statement:	This policy aims to provide NHS North East Hampshire and Farnham Clinical Commissioning Group staff with a structure within which to use the remote access systems and the portable devices which are available.
Responsibility for dissemination to new staff:	Line managers.
Training Implications:	Initial tuition on accessing the remote access systems
Further details and additional copies available from:	Governance Team
Equality Impact Assessment Completed?	The content of this policy does not raise any equality and diversity issues in relation to the protected characteristics
Consultation Process	Corporate Review Group Audit and Risk Committee
Approved by:	Corporate Review Group
Date approved:	11 January 2016

Intranet and Website Upload:

Intranet	Electronic Document Library Location:	
Website	Location in FOI Publication Scheme	Our Policies and Procedures
Keywords:	*Insert helpful keywords (metadata) that will be used to search for this document on the intranet and website*	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1		12	Review process amended to include CSU IG and ICT teams	November 2015
2		Throughout document	Amend CSU organisation name change to South, Central & West CSU	November 2015
3				
4				
5				

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
2.0	November 2015	Jackie Thomas, CSU IG Manager		Due for review November 2015

Contents

1. Introduction and Purpose

1.1 The developments within information technology have enabled NHS North East Hampshire and Farnham Clinical Commissioning Group (CCG) to adapt to more flexible and effective working practices, by providing portable computing and mobile devices to staff. CCG employees are now able to gain access to information and work systems from multiple locations, multiple devices and also remotely from home. It is important for all staff to understand the associated risks to the information, and the responsibility to ensure that information accessed remotely or held on portable devices, is protected by adequate security.

1.2 The purpose of this policy is to protect information that is processed remotely or is stored on portable devices. It forms part of an overall suite of information governance policies and should be read in conjunction with them, as well as the Information Security Policy.

2. Scope

2.1 This policy applies to all CCG staff who are entrusted with a supplied portable computing and data storage device, or who use any other portable computing and data storage device for the purposes connected with the work of the organisation. This policy also applies to staff working with the CCG information or accessing the organisation's network, remotely from a location which is not a routine work base, or using equipment that is not directly managed by the CCG IT providers. Employee compliance with this policy also covers:

- Connection to the CCG's network, which includes remotely and with portable devices;
- The processing of the CCG's information away from the organisation's premises;
- The secure transfer of information;
- The security of portable devices and information;
- The use of home computers and personal mobile phone and tablet services.

2.2 The CCG regards all identifiable information relating to patients as confidential.

2.3 The CCG regards all identifiable information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

2.4 All staff are required to comply with the Data Protection Act 1998, the Computer Misuse Act 1990, Health Records Act 1990 and the Common Law Duty of Confidentiality.

2.5 The organisation will make use of both confidential corporate information and patient or staff identifiable information. The following policy is applicable to both of these types of information except were specified differences apply. These differences are described throughout in policy.

3. Definitions

3.1 The use of portable computing and data storage devices includes:

- Laptops;

- Notebooks;
- Personal Digital Assistant (PDA);
- iPad/iPods/iPhones or other similar devices (tablets) capable of connecting (whether by a 'wired' or wireless connection) to a computing device and storing information;
- External portable Hard Disk Drives (HDDs);
- Smart mobile telephones capable of storing more than a basic phone book of contacts;
- USB Memory or 'Flash' Sticks and memory cards, capable of storing information;
- Solid state memory cards capable of storing information and being connected to the organisation's computing devices either by themselves or via another device;
- Media Supporting Storage which includes but not limited to:

    - Floppy Disks;
    - CD Disks, both recordable (CDR*) and Re-writable (CDRW*);
    - DVD/Blue-ray disks, both Recordable (DVDR*) and Re-Writable (DVDRW*);
    - Paper output from printers;
    - Zip disks and other magnetic tapes capable of recording and storing

3.2 Technology continues to evolve and thus this is not intended to be an exhaustive definition/list however, it includes all battery powered and mains adapted personal computing and storage devices.

3.3 **Remote working**

3.3.1 Remote working is accessing the organisation's resources whilst working away from normal fixed place of work, via any of the following:

- Mobile computing: Mobile computing is working at any location using mobile devices and/or removable data;
- Teleworking and homeworking: Working at home or any location other than your normal work base requiring periods of access to CCG information resources.
- Remote connection: Authorised staff can access data held on the organisation's secure server remotely using a strongly authenticated VPN (Virtual Private Network). The system allows access from any internet connected PC.

3.4 **Encryption**

3.4.1 Encryption is mandatory in all mobile devices used to store identifiable data. This was mandated as part of the Information Governance Assurance programme.

3.5 Unauthorised use and unauthorised access

3.5.1 Unauthorised use is when an individual accesses data or resources where they do not have a legitimate authority to do so. This includes sight of data, whether accidentally or deliberately.

4. Process/Requirements

4.1 Issue of Devices

4.1.1 Mobile Devices may be either:

- Issued by the organisation
- Provided by the individual

4.1.2 Regardless of whether the mobile device is issued by the organisation or provided by the individual, CCG staff will need to comply with organisation's IT Provider's Policies and Procedures as appropriate**.**

4.1.3 Sections 4.2 and 4.3 describe the controls and safeguards that apply to mobile devices provided by either the organisation or the individual. Section 4.4 describes the additional controls that will be applied to individual's mobile devices before they are allowed to connect to the organisation's network.

4.2 Physical Security

4.2.1 Staff shall accept full responsibility for the security of the portable devices issued to them, taking necessary precautions to avoid loss, theft or damage. In the event of loss, damage or theft, they must report this immediately to the assigned Data Custodian and in turn NHS South, Central and West CSU Head of Information Governance. In the event of the mobile device having been stolen, the incident should also be reported to the police and a crime reference number obtained.

4.2.2 All staff authorised to have portable devices **must**:

4.2.3 Take all reasonable care to prevent the theft or loss of this device. Any portable computing device is an attractive item and must not be left unattended in a public place or left in vehicles either on view, unattended or overnight. When transporting it, ensure that it is safely stowed out of sight.

4.2.4 Take extra vigilance if using any portable computing device during journeys on public transport to avoid the risk of theft of the device or unauthorised disclosure of the organisation's stored information by a third party "overlooking". There are security measures which can be deployed to support this if such travel is common to the role, staff should enquire through their line managers.

4.2.5 Not leave the device unattended for any reason unless the session is "locked" and it is in a safe working place, not left in an unattended publically accessible room for example. If it is anticipated leaving the device unattended it must be 'Logged Out' or 'Shutdown' to secure the device, if it is possible staff should take the device with them.

4.2.6 Ensure that other 'non' authorised users are not given access to the device or the data it contains.

4.2.7 Portable devices must be returned to the correct IT provider for a 'health check' at regular intervals as specified.

4.3 Passwords, Passphrases and Pin Codes

4.3.1 Passwords are an integral part of the Access Control mechanisms which are enforced by the Operating System (e.g. Windows). Network Passwords shall be a combination of letters and digits of a pre-determined length and combination of characters, typically using the lower case of the keyboard. Passwords and/or PINs should not normally be written down, but if unavoidable, are to be secured under lock and key at all times and never kept with the device or in an easily recognised form. Regular password changes reduce the risk of unauthorised access to the machine and therefore passwords must be changed at least every 60 days, but more frequently if required.

4.4 User-provided Mobile Devices

4.4.1 Home personal computers or laptops, must not be connected directly to the organisation's network.

4.4.2 Under special circumstances, and subject to prior testing and approval, smart phones or tablets may be connected to the organisation's network and may be used to store, process or transfer CCG information.

4.4.3 Use the User-supplied device request form to request the organisation's IT Provider to test the device if you want to connect your own mobile computing equipment to the organisation's network. The IT Provider will test the appliance, and if it is suitable to be connected they will apply the necessary software controls to the device and approve it for connection to the network. Any costs that are incurred in making your device suitable, such as encryption software and internet security, will be charged to your cost centre.

4.4.4 The mobile device will be technically unsupported, however the organisation's IT provider will make reasonable efforts to address any problems reported to them. In some cases, particularly to protect the organisation's data, data may be wiped from your device and the device may be reset to its factory settings.

5. Remote Working

5.1 Wireless and Cordless Computing Connections

5.1.1 Most of the latest portable devices are equipped with "Wireless" and other "Cordless" connection interfaces, Owners wishing to use the wireless interface(s) must request approval from the IT provider and subject to approval, cordless interfaces will only be enabled with organisation's approved protocol settings.

5.2 Wireless and Cordless Computing Precautions

5.2.1 Staff who intend to use portable devices with 'wireless' and other 'cordless' connection interfaces must comply with the organisations policies and procedures. For full details surrounding the necessary precautions, staff are asked to review the Information Security Policy.

5.3 Direct Connection to NHS North East Hampshire and Farnham CCG networks

5.3.1 Staff authorised to work from home or from other locations will need to use appropriate IT providers approved remote access solutions. These are secure internet connections which enables staff to gain access to the organisation's systems and information. Portwise/TIA will not allow staff to print or download documents unless working from an IT provider managed site.

5.3.2 All electronic processing devices connecting directly to the organisation's network (connected to a network point on NHS premises) must be protected by up to date anti-virus software. Where the device does not update automatically, it is the responsibility of the user to ensure that device is returned to the IT provider to enable a manual update of the anti-virus software.

6. Portable Computing Devices

6.1 The use of Portable Devices

6.1.1 Staff authorised to use portable devices must only use encrypted devices. Sensitive corporate and personal identifiable information must not be stored or transferred using any unencrypted "USB Memory" device. Non-sensitive or non-personal information may be stored and transferred using non encrypted "USB Memory" devices. Whilst the security of data is greatly increase when using encrypted "USB Memory" devices it does not remove responsibility from the user who must exercise due care and attention at all times when using these devices.

6.1.2 Where it is not possible to encrypt sensitive/personal information, the advice of the assigned Data Custodian and NHS South, Central and West CSU Information Governance Team is to be sought and, where no solution can be found, the risk is to be articulated to the Information Governance Steering Group for consideration.

6.1.3 Where available, only Connecting for Health approved encryption products are to be utilised to secure sensitive/personal information. Where no such products exists the advice of the assigned Data Custodian and the NHS South, Central and West CSU Information Governance Team is to be sought in all cases.

6.1.4 Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available. Information should not be stored permanently on portable devices. Always transfer documents back to their normal storage area as soon as possible. Failure to do so may result in problems with version control or loss of information if the portable device is lost or corrupted.

6.1.5 Staff must ensure that any suspected or actual breaches of security are reported to the assigned Data Custodian and the appropriate Head of Information Governance.

6.2 Information held on the Organisation's Portable Devices

6.2.1 Confidential information may only be held on the organisation's portable devices with the permission from the assigned Data Custodian. This should be recorded on a Service Information Asset Register and an updated copy sent to NHS South, Central and West CSU Information Governance Team.

6.2.2 Unauthorised software must not be installed onto the organisations portable devices with the exception of iPads that have been issued by the IT provider.

6.2.3 Information must be virus checked before transferring onto the organisations computers. This will be done automatically for information that is sent via email.

6.3 Use of Portable Devices by External Visitors

6.3.1 External visitors (lecturers, contractors, company representatives, etc.) may only connect portable devices, including USB sticks and laptops, to CCG assets where authorisation has been granted following consultation with the relevant IT provider.

6.3.2 Authorisation for the use of portable devices by external visitors will only be given following consultation with the It provider, they will ensure that the device is virus- scanned before any documents are opened.

6.4 Return of Portable Devices

6.4.1 Any owner leaving the organisation or no longer requiring use of an organisation's procured device must return the device to their line manager or the ICT Department. Line managers will be responsible for ensuring that any member of their staff having temporary ownership of

a device has returned it to them or the ICT Department before they leave the organisation. All media containing the organisation's information must be returned for retention or appropriate destruction.

7. iPads

7.1 The iPad is a very powerful mobile computing tablet and its power is enhanced by a host of readily available applications (apps) developed by 3rd parties. It is important to realise that these apps are not controlled by the NHS, and that data moved, manipulated or stored using these apps may not be secure and may contravene UK legislation. Guidance on use of apps can be provided by the relevant IT provider.

7.2 iPad Security controls

7.2.1 HITS have analysed the risks in using iPads and have introduced the following controls to help you ensure that the data you use remains safe. The responsibility for using and transferring the data safely while using the iPad remains with the user

Identified risk	Control
Loss/theft of iPad	The iPad can be wiped under the following circumstances: • User phones the help desk during normal working hours and reports the loss/theft of iPad • user can log onto web site if the iPad is lost or stolen outside normal working hours • The iPad automatically wiped after 5 unsuccessful attempts to enter the PIN code
Loading inappropriate apps	The organisation reserves the right to audit any mobile device that connects to the organisation's infrastructure. Refusals to submit to this audit are grounds for immediate cessation of all access rights, user IDs, and passwords from all devices connected to the network
Inappropriate usage	The organisation reserves the right to refuse, by physical and non-physical means, the ability to connect 'any mobile devices to the organisation's infrastructure. IT will engage in such action if it feels that the mobile device is being used in a way that puts the organisation's systems, data, users, and clients at risk.
Unauthorised data traffic	All employees who wish to connect mobile devices to network infrastructure other than the organisation's infrastructure to gain access to the organisation's data must employ an approved personal firewall and any other security measure deemed necessary by the IT department. The organisation's data is not to be accessed on any hardware that fails to meet these IT security standards.

8. Mobile Devices

8.1 Issue of Smart and Mobile Devices

8.1.1 IT provider authorises and issues Smart and mobile devices on behalf of the CCG

8.2 Use of Mobile Devices

8.2.1 It is important that the CCG demonstrates value for money in the use of mobile devices. Staff must provide assurance that the mobile devices are used appropriately at all times.

8.2.2 CCG staff should not under any circumstances use any mobile device whilst in control of a vehicle without an approved hands free kit.

8.2.3 All staff should be aware of their surroundings when using a mobile device, especially when discussing confidential information.

8.2.4 If a member of staff is given a device in order that they are contactable then their mobile device should be on at all times during business or 'on-call' hours, except when driving or when the user deems it inappropriate due to work reasons for example when in a meeting.

8.2.5 All CCG staff should take all reasonable measures to prevent loss, damage or theft.

9. Roles and Responsibilities

9.1 NHS North East Hampshire and Farnham Clinical Commissioning Group Chief Officer

9.1.1 The CCG Accountable Officer has overall responsibility for governance in the CCG. As accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

9.2 Caldicott Guardian

9.2.1 The CCG Caldicott Guardian has a responsibility for reflecting patients' interests regarding the use of personal identifiable information. They are responsible for ensuring all personal identifiable data is shared in an appropriate and secure manner and ensuring that appropriate information is made available to support patient care.

9.3 Senior Information Risk Officer (SIRO)

9.3.1 The CCG Senior Information Risk Officer (SIRO) is responsible for leading on the management of Information Risk and for overseeing the development of an Information Security Policy. For ensuring the Corporate Risk Management process includes all aspects of Information risk and for ensuring the CCG Executive Management Team (including the Senior management Team) is adequately briefed on information risk issues.

9.4 Information Security Expert

9.4.1 The Information Security expert within the associated IT provider is responsible, under a Service Level Agreement (SLA), for the implementation and enforcement of information security. The information security manager is also responsible for ensuring that the organisation is aware of its responsibilities and accountability for information security and for providing regular quarterly reports to the CCG Executive Management Team and Senior Management Team.

9.5 CCG Data Custodians

9.5.1 The Data Custodians within the CCG have the responsibility to provide assurance that information risk and the handling of information requirements are managed effectively. Data Custodians also have the responsibility to ensure staff compliance with policies and legislation/principles (Data Protection Act 1998, common law duty of confidentiality and Caldicott principles).

9.5.2 The Data Custodians will disseminate this policy and associated documentation to staff within their assigned department/directorate. Data Custodians must also ensure that information security applications to use remote working systems, portable computing and data storage resources, are approved.

9.6 CCG Employees

9.6.1 All staff, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of the legal and policy requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

9.6.2 All staff must abide by this and associated policies and procedures.

9.6.3 All staff should report any suspected breaches of this policy to their line manager or the assigned Data Custodian or NHS South, Central and West CSU Governance Team.

9.6.4 All staff must be aware and understand that failure to comply with the rules regulations contained within this policy, may result in disciplinary action.

10. Training

10.1 There is no formal training available for remote working systems, portable computing and data storage devices, however, the Information Governance Training Tool provides a module on **'Secure Transfer of Personal Data'**. This module will provide an insight securing personal/sensitive information using portable computing and data storage devices. CCG employees can find this IG module through the Information Governance Training Tool website:

11. Equality and Diversity and Mental Capacity Act

11.1 This policy was assessed against the CCG Impact Needs Requirement Assessment (INRA) tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities.

12. Success Criteria/Monitoring the Effectiveness of the Policy

12.1 The Corporate Review Group is responsible for the approval of this policy. The Audit and Risk Committee will then ratify that approval.

12.2 The Senior Information Risk Officer (SIRO), CSU Information Governance Team and Data Custodians are responsible for the implementation of this policy throughout the organisation.

12.3 Regular audits should be undertaken by Data Custodians to ensure that all portable computing and mobile devices issued can be accounted for and that assurance is provided to the Senior Information Risk Officer (SIRO) that identified risks are adequately controlled and managed.

12.4 Adherence to this policy will be monitored via investigation and analysis of information security incidents reported to the Information Governance Steering Group.

13. Review

This policy will be monitored by the South, Central and West CSU Information Governance Team in line with the CSU ICT policy to ensure any legislative changes that occur before the review date are incorporated. This document may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed biennially.

14. References and Links to other Documents

- CCG Information Governance Policy
- Information Security Policy
- Data Protection Policy
- Information Sharing Protocols