NHS
North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

Remote Working and Portable Devices Policy

As the South, Central & West Commissioning Support Unit (SCW) provides IT networks, equipment and support to North Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services information security policies. The following policy was developed by the CSU IT Services Team and adopted for use by the CCG.

This document can be made available in a range of languages and formats on request to the policy author.

Version:	2.1
Ratified by:	SCW CSU Corporate Governance Assurance Group
Date ratified:	29/11/2016
Name of Responsible Officer/author:	Andy Ferrari – Associate Director of IT Strategy and Planning
Name of responsible committee/individual:	IT Services Leadership Team
Name of executive lead:	Suzanne Tewkesbury – Director of Corporate Development & Performance
Date issued:	09/01/2018
Review date:	25/05/2018
Target audience:	All NHS South, Central and West CSU staff

Document Control Sheet

Title	**Remote Working & Portable Devices Policy**
Version	2.1
Status	Approved – Final
Author	Andy Ferrari
Date Created	29/12/2015
Date Last Updated	14/12/2017

History			
Version	Date	Author(s)	Comments
0.1	19/01/2016	Andy Ferrari	Initial SCW draft based on Stuart Collier's South CSU heritage document
1.0	02/02/2016	Andy Ferrari	Finalised – Updated following comments from SCW Information Governance Group and approval from SCW Corporate Governance Assurance Group
1.1	10/06/2016	Arif Gulzar	Updated: 4.1 to reflect personal devices must not connect to corporate network directly as per feedback from IG. Updated: 8.2 in line with Driving at work policy.
1.2a	06/09/2016	Arif Gulzar	Updated the policy review date
1.2b	04/10/2016	Arif Gulzar	Policy signed off by Information Governance Steering Group
2.0	29/11/2016	Arif Gulzar	Version reset after ratification from Corporate Governance Assurance Group
2.1	14/12/2017	Arif Gulzar	Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group

Approval/Sign Off	
Name	Title and contact
Philip Evans	Associate Director of IT Services
Catherine Dampney	CIO

Contents

1. INTRODUCTION & PURPOSE

1.1 The developments within information technology have enabled NHS South, Central and West CSU (CSU) to adapt to more flexible and effective working practices, by providing portable computing and mobile devices to staff. CSU 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

This policy applies to all CSU 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 CSU 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 CSU IT providers. Employee compliance with this policy also covers:

- Connection to the CSU's network, which includes remotely and with portable devices;
- The processing of the CSU'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.

The CSU regards all identifiable information relating to patients as confidential.

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

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.

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

The use of portable computing and data storage devices includes:

- Laptops;

- Notebooks;
- Personal Digital Assistant (PDA);
- Tablets and smartphones capable of connecting (whether by a ‘wired’ or wireless connection) to a computing device and storing information, and capable of storing more than a basic phone book of contacts;
- External portable Hard Disk Drives (HDDs);
- 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

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.

3.1 Remote working

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 CSU 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.

3.2 Encryption

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

3.3 Unauthorised use and unauthorised access

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

Mobile Devices may be either:

- **Managed Device**: Issued by the organisation
- **Personal Device**: Provided by the individual

Regardless of whether the mobile device is issued by the organisation or provided by the individual, CSU staff will need to comply with organisation's IT Services Policies and Procedures as appropriate**.** For mobile devices provided by the individual, all the conditions in section 4.4 must be fulfilled prior to access the information.

Any device provided by the individual must not be connected directly to the organisation's network.

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 indirectly to the organisation's network using the remote VPN solution.

4.2 Physical Security

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 the Head of Information Governance. In the event of mobile device having been stolen or lost, the incident must be logged on Datix system and also be reported to the police to obtain a crime reference number.

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

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.

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.

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.

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

4.3 Passwords, Passphrases and Pin Codes

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

Home personal computers or laptops, must not be connected directly to the organisation's network. The storage of CSU information on user provided devices is strictly prohibited.

Compatible Personal portable devices (e.g. Tablet / Smartphone) may be used to access web-based resources however the SCW security policy will be enforced:

- Pin code will be enabled
- Device encryption is required
- All data (*) will be removed from the device if the pin is entered incorrectly 5 times.

(*) This includes all personal information on the device (e.g. Contacts, Photographs, and Messages). SCW CSU cannot be held responsible for the loss of personal data if the security policy is actioned (e.g. deletion following 5 pin attempts).

5 REMOTE WORKING

5.1 Wireless & Cordless Computing Connections

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 IT Services and subject to approval, cordless interfaces will only be enabled with organisation's approved protocol settings.

5.2 Wireless & Cordless Computing Precautions

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 South, Central and West CSU networks

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. These remote access solutions will not allow staff to print or download documents unless working from a site where SCW manage IT Services.

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 IT Services to enable a manual update of the anti-virus software.

6 PORTABLE COMPUTING DEVICES.

6.1 The use of Portable Devices

Staff authorised to use portable devices must only use encrypted devices. Information must not be stored or transferred using any unencrypted "USB Memory" device. 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.

Where it is not possible to encrypt sensitive/personal information, the advice of the assigned Data Custodian and Information Governance Team is to be sought and, where no solution can be found, the risk is to be articulated to the CSU Executive Management Team for consideration.

Only encryption products approved by SCW are to be utilised to secure sensitive/personal information. Where no such products exists the advice of the assigned Data Custodian and the Information Governance Team is to be sought in all cases.

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.

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

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 the Information Governance Team.

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

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

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

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

6.4 Return of Portable Devices

Any owner leaving the organisation or no longer requiring use of a SCW procured device must return the device to their line manager or IT Services. 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 IT Services before they leave the organisation. All media containing the organisation's information must be returned for retention or appropriate destruction.

7 Tablets

Tablets are very powerful mobile computing devices and their 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 provider.

7.1 Tablet Security controls

SCW CSU IT Services have analysed the risks in using tablets and have introduced the following controls to help staff ensure that the data used remains safe. The responsibility for using and transferring the data safely while using the tablet remains with the user

Identified risk	Control
Loss/theft of iPad	The tablet can be wiped under the following circumstances: User phones the help desk during normal working hours and reports the loss/theft of tablet. The tablet is 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 Services 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 IT Services. 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

IT provider authorises and issues Smart and mobile devices on behalf of SCW

8.2 Use of Mobile Devices

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

It is against the law to manually operate any mobile device whilst driving or riding a vehicle. As set forth in its Health and Safety Policy, SCW holds the following official position with regard to the use of hands-free mobile phone equipment:

Hands-free kits for mobile phones are legal to use, however, a telephone conversation using hands-free is a significant distraction. Therefore, whilst driving for work, employees should use their hands-free mobile phone only when absolutely necessary. Drivers must retain full use of their vehicles at all times, and any calls made to and from a hands-free mobile should be kept as short as possible. Staff may not call in to meetings whilst driving and meeting Chairs are expected to tell anyone doing so to hang up and dial-in once legally and safely parked with the engine switched off. The SCW Health and Safety Policy and Procedure for Driving at Work are available on 'The Nest'.

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

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.

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

9 ROLES & RESPONSIBILITIES

9.1 NHS South, Central and West CSU Managing Director

The SCW Managing Director has overall responsibility for governance in the CSU. 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

The SCW 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 NHS South, Central and West CSU Senior Information Risk Officer (SIRO)

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

9.4 Information Security Expert

The Information Security expert within SCW IT Services 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 SCW Executive Management Team.

9.5 NHS South, Central and West CSU Data Custodians

The Data Custodians within the CSU 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).

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 NHS South, Central and West CSU Employees

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.

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

All staff should report any suspected breaches of this policy to their line manager or the assigned Data Custodian or Information Governance Team.

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

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. CSU employees can find this IG module through the Information Governance Training Tool website:

11 Equality and Diversity and Mental Capacity Act

This policy was assessed against the CSU 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

The Information Governance Steering Group is responsible for the approval of this policy. The Corporate Business Committee will then ratify that approval.

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

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.

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

13 Review

The CSU Executive Management Team is responsible for the review of this policy.

14 References and Links to other Documents

SCW Information Governance Policy
Information Security Policy
Data Protection Policy
Information Sharing Protocols