NHS
West Hampshire
Clinical Commissioning Group

REMOTE WORKING AND PORTABLE DEVICES SECURITY POLICY

Version 3

Subject and version number of document:	Remote Working and Portable Devices Security Policy Version 3
Serial number:	COR/049/V3.00
Operative date:	1 December 2019
Author:	CSU IT Services
CCG owner:	Senior Information Risk Owner
Links to other policies:	• Information Incident Management & Reporting Procedure • Information Governance Management Framework and Strategy and associated policies • Information Security Policy • Clear Screen & Desk Policy • Access Control Policy • Provision of Mobile Devices Policy
Review date:	October 2021
For action by:	All Staff
Policy statement:	This policy supports staff in compliance with Data Protection legislation, achieving best practice in processing information remotely in a secure way using portable devices.
Responsibility for dissemination to new staff:	Line managers at induction.
Mechanisms for dissemination:	All new and revised policies are promoted through the staff newsletter / intranet and published on the CCG website.
Training implications:	All staff should be made aware of where to find CCG policies at induction.
Resource implications	There are no resource implications in relation to this policy.
Further details and additional copies available from:	Website: https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Equality analysis completed?	This policy has been assessed as having a low impact on people with characteristics protected by the Equality Act. As such a full equality impact assessment is not required.
Consultation process	CSU IG Steering Group CSU Corporate Governance Assurance Group

	CCG Policy Sub Group
Approved by:	Policy Sub Group
Date approved:	13 November 2019

Website Upload:

Website	Location in FOI Publication Scheme	https://www.westhampshireccg.nhs.uk/documents?media_folder=193&root_folder=Information%20governance%20(IG)%20and%20security
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	Dec 16		Sections 4.1, 8.1 and 8.2 amended and policy re-badged as a CCG policy.	Dec 16
2	Nov 17	11, 12 and 15	Amendments throughout to references to SCW CSU IT to reflect that this is now a CCG corporate policy, section 4.4.2 to make it more clear and relevant as per NHSmail acceptable use policy, that risks regarding transfer of data would now be articulated to the Audit Committee, rather than the Finance & Assurance Committee and to update the application process for mobile devices in line with current procedure.	Nov 17
3	Feb 19		Complete re-write. Policy based on SCW CSU policy version 2.2. Renamed Remote Working and Portable Devices 'Security' Policy to help differentiate with Provision of Mobile Devices Policy.	

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
2	Sept 16	CSU IT / CCG Policy Administrator	Policy Sub Group / Board November 2016	See amend 1 above
2.1	Sept 17	CSU IT	Policy Sub Group / Board November 2017	See amend 2 above
3	Feb 19	CSU Cyber Security Manager	Policy Sub Group	See amend 3 above

REMOTE WORKING & PORTABLE DEVICES SECURITY POLICY

SUMMARY OF KEY POINTS TO NOTE

This policy supports staff in compliance with Data Protection legislation, achieving best practice in processing information remotely in a secure way using portable devices.

- Regardless of whether a mobile device is issued by the CCG or provided by an individual, employees will need to comply with the South Central & West Commissioning Support Unit (SCW CSU) core IT policies as adopted by the CCG, CCG IT security policies and CCG information governance policies.
- Only encrypted portable devices may be used and they 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.
- Any loss, damage or theft of portable devices should be reported to the team Information Asset Owner. In addition the CSU IT service desk must also be informed to determine if any immediate action is required, such as remotely wiping the device.
- Portable devices must not be left unattended in a public place or left in vehicles either on view, unattended or overnight. When transporting it, ensure it is safely stowed out of sight. Take extra vigilance if using portable devices during journeys on public transport to avoid the risk of theft of the device or unauthorised disclosure of information by a third party 'overlooking'.
- Staff **MUST NOT** charge mobile devices by plugging into USB ports on CCG / SCW CSU supported desk top PCs or laptops. This is in order to prevent any data leakage and applies to all mobile equipment, including individuals' personal devices and those supplied by the CCG / CSU.
- If you are accessing your NHSmail account from a non-NHS device (i.e. a home computer, personally owned laptop or in an internet café) you should only access the service via a web browser at www.nhs.net and not through a third party email programme configured on the device such as Microsoft Outlook as per the NHSmail acceptable use policy. This is because if a security breach should occur because of that access, SCW CSU IT Services will not be responsible.

REMOTE WORKING & PORTABLE DEVICES SECURITY POLICY

Contents

REMOTE WORKING & PORTABLE DEVICES SECURITY POLICY

1. INTRODUCTION AND PURPOSE

1.1 The developments within information technology have enabled the CCG to adapt to more flexible and effective working practices, by providing portable computing and mobile devices to staff. Authorised staff 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.

1.3 This policy aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft
- Accidental or deliberate overlooking by unauthorised individuals
- Unauthorised access to PROTECTED and RESTRICTED information
- Unauthorised introduction of malicious software and viruses
- Potential sanctions against the organisation or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse
- Potential legal action against the organisation or individuals as a result of information loss or misuse
- Reputational damage for the organisation as a result of information loss or misuse.

2. SCOPE AND DEFINITIONS

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's information or accessing the organisation's corporate data network, remotely from a location which is not a routine work base, or using IT equipment that is not directly managed by NHS South, Central & West Commissioning Support Unit (SCW CSU) IT. Staff compliance with this policy also covers:

- Connection to the corporate data 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 data or information
- The security of portable devices and information
- The use of home computers and personal mobile phone and tablet devices.

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. Please see the guidance in the table below:

Personal Data (derived from the General Data Protection Regulation (GDPR))	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).

Commercially Confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

Legal Compliance Guide

2.4 The legal framework on which this policy and other related information security policies are based is as follows.

2.5 All CCG staff are required to ensure compliance with Data Protection Legislation. This includes:

- General Data Protection Regulation (EU) 2016/679 (GDPR)
- Data Protection Act (DPA) 2018
- Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws, implementing them as amended from time to time.

2.6 In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality and the processing and sharing of personal data including:

- Human Rights Act 1998
- Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015
- Common Law Duty of Confidentiality
- Privacy and Electronic Communications (EC Directive) Regulations

2.7 Consideration must also be given to the:

- Computer Misuse Act 1990 and as amended by the Police and Justice Act 2006 (Computer Misuse)
- Copyright, Designs and Patents Act 1998
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Health Records Act 1990
- Fraud Act 2006
- Bribery Act 2010
- Criminal Justice and Immigration Act 2008
- Equality Act 2010

- Terrorism Act 2006
- Malicious Communications Act 1988
- Digital Economy Act 2010 and 2017
- Counter-Terrorism and Security Act 2015.

2.8 This legislation can be accessed via the following link: http://www.legislation.gov.uk/

Definitions

2.9 The use of portable computing and data storage devices includes but is not limited to:

- Laptop computers
- Tablets or other hand-held devices
- Smartphones including Android and iPhones which are 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 is not limited to:
    - 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 information.

2.10 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.

2.11 **Remote working**

2.11.1 Remote working is accessing the organisation's network resources whilst working away from the 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 the CCG's information resources
- **Remote connection**: Authorised staff can access data held on the organisation's secure server remotely using a multi-factor authentication encrypted VPN (Virtual Private Network). The system allows access to authorised staff to the corporate data network from CCG / CSU provided internet connected computers (i.e. not personal devices).

2.12 **Encryption**

2.12.1 Encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version, to make it unreadable by unauthorised users, which can only be decoded by authorised users.

2.13 **Unauthorised use and unauthorised access**

2.13.1 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. Staff members can be personally prosecuted where data is accessed outside of their normal working activities without the legitimate authority to do so.

3. POLICY STATEMENTS

3.1 It is the responsibility of staff to ensure that the following policy statements are adhered to at all times whilst they are responsible for SCW CSU managed portable computing devices i.e. devices that are managed and supported by SCW IT services:

3.2 Encryption & Removable Media

3.2.1 All portable computing devices capable of storing data **MUST** be protected by a full disk encryption solution approved to protect the identified data security classification. Approved encryption solutions include solutions that can be used by the Government and Public Sector which are listed on the NCSC (National Cyber Security Centre) website.

3.2.2 All removable media **MUST** be encrypted or individual files/directories copied to the removable media **MUST** be encrypted with an appropriate encryption solution approved to protect the security classification of the information on the media. For USB sticks, the approved standard is AES256 bit encryption with FIPS 140-2.

3.2.3 Staff MUST ensure that portable computing devices (laptops, smartphones, tablets and USBs) are encrypted where these are not covered in the SCW CSU IT core service level agreement.

3.2.4 In the event that a full disk encryption solution has not been, or cannot be, configured on the device then the risks to the information **MUST** be assessed and either:

- An alternative encryption solution **MUST** be utilised for which the risks have been accepted by the relevant Information Asset Owner (IAO), and if required the Senior Information Risk Owner (SIRO); or
- The device remains unencrypted and the risks **MUST** be qualified and accepted by the relevant IAO, and if required the SIRO.

3.3 Configuration and Asset Management

3.3.1 Staff **MUST NOT** install any software on to the portable computer device unless authorised and approved by the IT Service Desk.

3.3.2 Staff **MUST NOT** change the configuration of any portable computer device.

3.3.3 Staff **MUST NOT** remove or deface any asset registration number.

3.3.4 Staff **MUST NOT** install any hardware to or inside any portable computer device, unless authorised by the IT Services Desk.

3.3.5 Staff **MUST NOT** charge mobile devices by plugging into USB ports on CCG / SCW CSU supported desk top PCs or laptops. This is in order to prevent any data leakage and applies to all mobile equipment including individuals' personal devices and those supplied by the CCG / CSU.

3.3.6 Staff **MUST** allow SCW CSU IT Services access to the portable computer device to undertake any maintenance work.

3.3.7 Any documents downloaded onto portable devices should be deleted on a regular basis.

3.3.8 Staff accessing the Continuing Healthcare patient system from a mobile device should change the default folder for downloads to the personal drive. Where this is not possible, downloads which have been stored on the device should be deleted on a weekly basis to avoid any Personal Confidential Data (PCD) breaches; each document opened and viewed in the patient system automatically stores a copy on the device's download file which can lead to PCD being unintentionally stored and may cause the device to slow down.

3.3.9 Staff should seek advice from the IT Service Desk before taking any CCG / SCW supplied IT equipment outside the United Kingdom.

3.3.10 IT Services may at any time, and without notice, request a software or hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. IT Services will provide the user with alternative equipment during this time. All staff **MUST** co-operate fully with any such audit.

3.4 Data Storage

3.4.1 Data **MUST** be stored on the corporate network only and not held on portable devices.

3.4.2 Staff **MUST NOT** store any data on non-CCG / SCW supplied devices. This applies to home PCs or PCs used in hotels or internet cafes.

3.4.3 Staff **MUST NOT** store data on diskette, CD or other similar storage device.

3.5 Portable / Removable Media Drives

3.5.1 Portable media includes but is not limited to Memory / USB Sticks, External Hard Drives, SD Cards, CDs, Diskettes and Floppy Drives.

3.5.2 Portable media drives information when other more secure methods are not available. Information **MUST 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.

3.5.3 Where there is legitimate requirement to store data for secure transfer using portable media drive then use ONLY a CCG / SCW CSU-supplied encrypted memory stick. Please refer to the CCG's Provision of Mobile Devices Policy, which sets out the criteria against which staff are measured for eligibility for a mobile IT device, along with the authorisation process.

3.5.4 Each encrypted memory stick has a unique serial number and password. Information cannot be accessed unless the password is known. Do not write the password down, and if it needs to be shared with other members of staff, inform the other individual verbally.

3.5.5 Memory sticks should not be labelled with any sort of NHS identification. They are secure, and without the password they are useless. It should not be possible to determine that the memory stick is the property of the NHS.

3.5.6 Personal memory sticks MUST not be plugged into any corporate endpoints i.e. laptop, workstation, server, printer or any network equipment unless authorised by the Service Desk.

3.6 Access Control

3.6.1 SCW CSU IT Services will provide appropriate security measures to allow remote users to access corporate systems by connecting over public networks such as the internet.

3.6.2 Staff **must** only access the corporate network and information systems through SCW CSU IT approved remote access VPN solutions.

3.6.3 Users should ensure portable computer devices are logged off, or the keyboard locked when left unattended, even if only for a few minutes. Please see Clear Screen & Desk Policy for further guidance.

3.6.4 **Under no circumstances** should PROTECTED or RESTRICTED information be emailed to your personal non-NHSmail email address.

3.7 Physical security

3.7.1 Staff should take all reasonable care to prevent the theft or loss of mobile devices. 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.

3.7.2 Staff should 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.

3.7.3 Staff should 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.

3.7.4 Staff must ensure that other 'non-authorised' users are not given access to the device or the data it contains.

3.8 Antivirus Protection

3.8.1 IT Services will deploy an up-to-date antivirus signature file and security updates for applications and software to all managed laptops.

Staff working remotely **MUST** ensure that their laptops are regularly connected to the corporate network (via VPN) to enable the antivirus software to be updated and operating system security updates to be applied.

3.9 Passwords, Passphrases and Pin Codes

3.9.1 Passwords are an integral part of the access control mechanisms which are enforced by the operating system, (for example, Microsoft Windows). Network passwords **MUST** be a combination of letters and digits of a pre-determined length and combination of characters. Passwords and / or PINs MUST not 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.

3.10 Personal Devices / BYOD (Bring Your Own Device)

3.10.1 Home personal computers or laptops **MUST NOT** be connected directly to the organisation's network i.e. physically plugged into the network. The storage of the CCG's information / data on personal devices is strictly prohibited.

3.10.2 The Continuing Healthcare database Care Track should not be accessed by personal devices and only through NHS provided devices.

3.10.3 If you are accessing your NHSmail account from a non-NHS device (i.e. a home computer, personally owned laptop or in an internet café) you should only access the service via a web browser at www.nhs.net and not through a third party email programme configured on the device such as Microsoft Outlook as per the NHSmail acceptable use policy. This is because if a security breach should occur because of that access, SCW CSU IT Services will not be responsible.

3.10.4 Usage of the CCG's guest Wi-Fi is primarily for business use. Occasional and reasonable personal use is permitted on personal mobile devices, for example during lunch breaks, provided that such use does not interfere with performance of duties and does not conflict with CCG policies, procedures and contracts of employment.

3.10.5 All employees who wish to connect their personal mobile devices to the guest Wi-Fi should enable their personal firewall and any other security measures in order to protect their own devices. The organisation's data is not to be accessed on any hardware that fails to meet SCW CSU IT security standards.

3.11 Wireless and Cordless Computing Connections

3.11.1 Most of the latest portable devices are equipped with "wireless" and other "cordless" connection interfaces. Staff wishing to use the

wireless interface(s) **MUST** request approval from the IT Service Desk and subject to approval, cordless interfaces will only be enabled with the organisation's approved protocol settings.

3.11.2 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 and comply with the Information Security Policy.

3.12 Use of USBs by external visitors

3.12.1 External visitors (lecturers, contractors, company representatives, etc.) may only connect USB sticks to corporate managed assets where authorisation has been provided following consultation with SCW CSU IT Service Desk.

3.12.2 Authorisation for the use of USB sticks by external visitors will only be given following consultation with the IT Service Desk; they will ensure that the device is virus-scanned in a controlled environment (Sandbox) before it is plugged in to any managed device on the corporate network and any documents stored on it are opened.

4 TABLETS AND SMARTPHONES

4.1 Tablets and smartphones are very powerful mobile computing devices and their power is enhanced by a host of readily available applications (apps) developed by third parties, some of which are core apps that are pre-installed and are integral to the function of the device. It is important to realise that these apps are not controlled by the CCG / SCW CSU, and that data moved, manipulated or stored using these apps may not be secure and may contravene UK legislation. Guidance on the use of apps can be provided by the relevant application provider. Third party applications such as Facebook, LinkedIn, Instagram, Twitter and Nexus Trul can be installed subject to all the conditions in section 4.4.

4.2 Any apps installed on CSU / CCG provided devices not listed above may need to be deleted; please seek advice from IT services.

4.3 There is software available which can be installed to support staff with a disability; this should be discussed with line managers / IT services and agreed on a case by case basis.

4.4 Tablet and smartphone security controls

4.4.1 SCW CSU IT services have analysed the risks in using tablets and smartphones 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 or smartphone remains with the user.

Identified risk	Control
Loss / theft of tablet / smartphone	The tablet or smartphone can be wiped under the following circumstances: User rings IT service desk during normal working hours and reports the loss/theft of tablet/ smartphone. When configured with NHSmail, the tablet/smartphone is automatically wiped after 5 unsuccessful attempts are made while entering the PIN code. The lost/stolen tablet/ smartphone can also be wiped off using the NHSmail portal i.e. Email->Settings->Options->phone.
Loading inappropriate apps	The organisation reserves the right to audit any tablet/ smartphone device that connects to the organisation's corporate 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. The CCG reserves the right to audit 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 CCG receives itemised bills for mobile devices and monitors unusually high usage which is referred to the appropriate line manager for review. Deliberate misuse will be considered in accordance with the current Local Anti-Fraud Bribery and Corruption Policy, along with the Conduct, Performance, Grievance & Absence Management Policy. Refer to Provision of Mobile Devices Policy.
Unauthorised data traffic	All employees or visitors who wish to connect unmanaged (by SCW CSU IT Services) mobile devices to network infrastructure other than the organisation's infrastructure to gain access to the guest wi-fi should enable their personal firewall and any other security measures deemed necessary by IT Services in order to protect their own devices. This is because guest wi-fi is not monitored by IT services, who would not be responsible if mobile devices are infected by a virus / ransomware etc. The organisation's data is not to be accessed on any hardware that fails to meet these IT security standards.

4.5 Issue of smart and mobile devices

4.5.1 Please refer to the CCG's Provision of Mobile Devices Policy, which sets out the criteria against which staff are measured for eligibility for a mobile IT device. The application form as specified within the policy should be provided to the CCG admin team for submission to the chief finance officer or nominated deputy for approval.

4.5.2 Once authorised, the CCG IT provider will arrange the supply of the device.

4.6 Use of mobile devices (tablets and smartphones)

4.6.1 It is pertinent to note that the CCG demonstrates value for money in the usage of smartphones and tablets. Staff **MUST** ensure that these devices are used appropriately at all times.

4.6.2 In accordance with the CCG's Health & Safety Policy in regard to mobile communications, the CCG expects all employees to obey the law i.e. not to drive whilst using a hand-held mobile phone. If a call comes in whilst driving, the standard course of action should be to wait until reaching a safe stopping area, switch off the engine, and then take the message / call back as appropriate. There is currently no national ban on the use of 'hands-free' or other devices such as satellite navigation, but staff are strongly advised to adhere to the manufacturers / suppliers guidance on their safe use during a car journey.

4.6.3 All staff should be aware of their surroundings when using a mobile device, especially when discussing personal and / or sensitive information.

4.6.4 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.

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

5. ROLES AND RESPONSIBILITIES

5.1 Accountable Officer

5.1.1 The accountable officer has overall responsibility for information governance in the CCG. As accountable officer they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The management of information risk and information governance

practice is now required within the Statement of Internal Control which the accountable officer is required to sign annually.

5.2 Senior Information Risk Officer (SIRO) *

5.2.1 The senior information risk officer (SIRO) has been allocated lead responsibility for the CCG's information risks and provides the focus for management of information risk at executive management level. The SIRO must provide the accountable officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. The SCW CSU information governance team will support the SIRO in fulfilling this role.

5.3 Caldicott Guardian *

5.3.1 The Caldicott guardian has overall responsibility for protecting the confidentiality of information that includes personal data and special categories of personal data, and for ensuring it is shared appropriately and in a secure manner. The role has the responsibility to advise the CCG Executive Team on confidentiality issues. The SCW CSU information governance team will support the Caldicott guardian in fulfilling this role.

5.4 Data Protection Officer *

5.4.1 The CCG data protection officer (DPO) has the responsibilities as set out in the GDPR guidance, such as monitoring compliance with IG legislation, providing advice and recommendations on DPIAs, giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the Information Commissioners Office (ICO).

**Details of the current leads within the CCG can be found on the Information Governance page of the intranet.*

5.5 SCW Deputy Data Protection Officer

5.5.1 The SCW deputy data protection officer (DDPO) is the person within SCW that has been identified to support the role of the Data Protection Officer (DPO) in NHS England. This role has the responsibilities as set out in the GDPR guidance as delegated duties from the DPO and is responsible to feedback any information governance issues to SCW Executive Management Team and the DPO at NHS England. The DDPO will ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO is informed no later than 72 hours after the organisation becomes aware of the incident. They will also be part of the Data Protection Impact Assessment (DPIA) process on behalf of SCW.

5.6 SCW Information Governance Team

5.6.1 The SCW information governance team is responsible for ensuring that the information governance programme is implemented throughout the organisation. The team is also responsible for the completion and annual submission of the Data Security and Protection Toolkit on behalf of the CCG. The information governance team will support the organisation in investigating Serious Incidents Requiring Investigation (SIRIs), offer advice and ensure the organisation complies with legislation, policies and protocols. The information governance team will provide local face-to-face IG training if required and will monitor staff compliance by way of the consult OD portal and link to the e-LfH platform.

5.7 Information Asset Owners (IAO)

5.7.1 The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what data and information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The information governance team will support the IAOs in fulfilling their role.

5.8 Data Custodians (DCs) / Information Asset Administrators (IAAs)

5.8.1 Data custodians are required to support the IAO's and SIRO who will work with the information governance team to ensure staff apply the Data Protection Legislation and Caldicott Principles within working practices.

5.9 SCW Cyber Security Manager

5.9.1 Responsibilities of the Cyber Security Manager include:

- Acting as a central point of contact on IT security within the organisation and for external organisations (such as West Hampshire CCG) that have entered into an agreement for the provision of IT services by the CSU
- Implementing an effective framework for the management of security
- Assisting in the formulation of the Information Security Policy and related policies
- Advise on the content and implementation of the Information Security Programme
- Co-ordinate IT security activities particularly those related to shared information systems or IT infrastructures
- Liaise with external organisations on IT security matters, including representing the organisation on cross-community committees

- Advising users of information systems, applications and networks of their responsibilities
- Creating, maintaining, giving guidance on and overseeing the implementation of IT security
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk
- Ensure breaches of policy and recommended actions are reported in line with organisation's procedures.

5.10 Line Manager Responsibilities

5.10.1 Line managers **MUST** inform the IT Service Desk of any authorised remote workers and the systems they require access to via the SCW IT Support Portal.

5.10.2 Any user leaving the organisation or no longer requiring use of a CCG procured device must return the device to their directorate PA as per the leavers process; for Continuing Healthcare (CHC) staff this will be to the CHC business support team (refer to Provision of Mobile Devices Policy). Line managers will be responsible for ensuring that any member of their staff having temporary ownership of a device has returned it before they leave the organisation. All media containing the organisation's information must be returned for retention or appropriate destruction.

5.11 Staff

5.11.1 Staff **MUST** immediately report any faults with, or damage to the portable computer device, to the IT Service Desk.

5.11.2 Staff **MUST** ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above points, the CCG / SCW IT may recover the costs of repair.

5.11.3 Staff **MUST** 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 IT Service Desk and their team departmental Information Asset Owner to report on Datix, following which the CSU IG team will investigate / action as appropriate (please refer to the CCG Information Incident Management & Reporting Procedure). The team data custodian / information asset administrator (IAA) should also be notified to ensure that the information asset register is updated as appropriate.

5.11.4 In the event of a mobile device having been stolen or lost, the incident must be logged on the Datix system and also be reported to the police

to obtain a crime reference number. The IT service desk should also be notified so that they can take any immediate action, such as remotely wiping the device.

5.11.5 Staff **MUST** ensure that appropriate security (Physical and Logical) measures are taken to stop unauthorised access to any information, either on the portable computer device or in printed format. Staff are bound by the same requirements on confidentiality and Data Protection as the organisation itself.

5.11.6 Mobile devices (smartphones and tablets), that are not protected by mobile device management solution, should be kept up to date with the latest software available via the manufacturer.

5.11.7 All staff **MUST** report any suspected or actual breaches of security to their line manager or the assigned Information Asset Owner.

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

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

5.11.10 Under the General Data Protection Legislation when a serious incident resulting in the unlawful loss or disclosure of personal data is reported, cooperation with the Information Commissioner's Office (ICO) may be required. Staff should contact their Information Asset Owner to consider whether the incident should be reported on Datix. Advice may also be sought from the CCG Data Protection Officer or the SCW CSU information governance team.

6. TRAINING

6.1 There is no formal training available for remote working systems, portable computing and data storage devices. However, all staff are required to complete training using the NHS Data Security Awareness Level 1 modules provided by NHS Digital via the e-LfH platform, accessible through ConsultOD, or approved face-to-face training if offered. This training tool provides a module on 'Secure Transfer of Personal Data' which will provide an insight on securing personal/sensitive information using portable computing and data storage devices https://nhsdigital.e-lfh.org.uk/.

7. EQUALITY AND DIVERSITY

7.1 The CCG is committed to equality, diversity and inclusion for all, as well as to meeting the Public Sector Equality Duty (Equality Act 2010).

7.2 Both new policies, and existing policies when reviewed, come within the Public Sector Equality Duty. This means that policy authors must consider

whether the policy will be effective for all patients and / or staff. This process is called equality impact assessment.

7.3 This policy has been assessed as having a low impact on people with characteristics protected by the Equality Act. As such a full equality impact assessment is not required.

8. SUCCESS CRITERIA / MONITORING THE EFFECTIVENESS OF THE POLICY

8.1 The CCG Policy Sub Group is responsible for the approval of this policy.

8.2 The SIRO, CSU information governance team and data custodians / IAAs are responsible for ensuring the implementation of this policy throughout the organisation.

8.3 Regular audits are undertaken by data custodians / IAAs to ensure that all portable computing and mobile devices issued can be accounted for and that assurance is provided to the SIRO that identified risks are adequately controlled and managed.

8.4 Adherence to this policy will be monitored via investigation and analysis of information security incidents reported to the Audit Committee.

9. REVIEW

9.1 This document may be reviewed at any time at the request of either the Staff Forum or management, or in response to changes in legislation, but will automatically be reviewed on a biennial basis.

10. REFERENCES AND LINKS TO OTHER DOCUMENTS

- CCG Information Governance Management Framework and Strategy and associated policies
- Information Security Policy
- Clear Screen & Desk Policy
- Access Control Policy
- CCG Information Incident Management & Reporting Procedure
- Provision of Mobile Devices Policy
- Information Security Management: NHS Code of Practice
- NHS Records Management: Code of Practice