NHS
Surrey Downs
Clinical Commissioning Group

Remote Working and Portable Devices Policy

Policy ID	IG04
Version:	V2.0
Author	Interim IG Manager
Last review date:	27th July 2015
Next review date:	1st August 2017
Date agreed by	25th August 2015 (Executive Committee)

Improving care together across Surrey Downs

Summary

The Policy sets out minimum standards and safe working practices for all CCG. The purpose of this policy is to protect information that is processed remotely or stored on portable devices. This Remote Working Portable Devices Policy aims to allow staff to use technology to work in flexible manner that is mutually beneficial to themselves and the CCG. The policy sets out to achieve the following:

Version History

Version	Review Date	Name of Review	Ratification Process	Notes
1.0	29/09/2013	NHS South CSU IG Team	Final	CCG Governing Body
1.1	22/07/2015	Interim IG Manager – Surrey Downs CCG	Draft	Reviewed and updated to reflect to reflect recent IG Toolkit guidelines and accountability and responsibility in the CCG.
2.0	25/08/2015	Interim IG Manager – Surrey Downs CCG	Final	Approved by Executive Committee
Contributors		Governing Body Secretary, Head of Planning & Performance and, South East CSU Information Governance Principle Associate.		
Audience		All CCG officers, Governing Body members and staff (which includes temporary staff, contractors and seconded staff) and CCG members in their capacity as commissioners.		

Equality Statement

Surrey Downs Clinical Commissioning Group (Surrey Downs CCG) aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Human Rights Act 1998 and promotes equal opportunities for all. This document has been assessed to ensure that no-one receives less favourable treatment on grounds of their gender, sexual orientation, marital status, race, religion, age, ethnic origin, nationality, or disability.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the person requesting has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

Surrey Downs CCG embraces the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

Equality Analysis

This policy has been subject to an Equality Analysis, the outcome of which is recorded below.

1. Does the document/guidance affect one group less or more favourably than another on the basis of:			
	• Race	Yes, No or N/A	Comments
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	No	
4	Is the impact of the document/guidance likely to be negative?	N/A	
5	If so, can the impact be avoided?	N/A	
6	What alternative is there to achieving the document/guidance without the impact?	N/A	
7	Can we reduce the impact by taking different action?	N/A	

Contents

1. Introduction

Remote working is an increasingly important part of Surrey Downs Clinical Commissioning Group's (the CCG) strategy to boost productivity, collaboration and access to critical information assets. This Remote Working and Portable Devices Policy is intended to give all staff, clarity about work expectations and responsibilities and to provide guidance on the provision of suitable portable devices.

The intention of this policy is not to be explicit in daily duties, but informs staff and managers of the reasonable expectations of staff who may attend the office less frequently and the expectations that staff should have of the CCG. The policy does not specify groups of staff who may or may not be eligible for allocation of a CCG funded device, but provides guidance for an agreement between staff and their line managers of a suitable remote working arrangement. It also recommends a range of available devices and defines what technical support is available to staff using either their own mobile devices or those provided by the CCG.

This policy applies to staff directly employed by, or working under a temporary contract with the CCG requiring access to the CCG network.

In line with the existing contract/Service Level Agreement/s (SLAs) the Information Communication Technology (ICT) department/directorate within South East Commissioning Support Unit (the CSU) is responsible for managing ICT services on behalf of the CCG. All staff should ensure that they have read the CSU's procedure/s on remote working as a condition of the CSU providing remote access to the CCG's network. As such, this policy contains wording from the CSU remote working procedure/s.

2. Purpose

The purpose of this policy is to protect information that is processed remotely or stored on portable devices. This Remote Working Portable Devices Policy aims to allow staff to use technology to work in flexible manner that is mutually beneficial to themselves and the CCG. The policy sets out to achieve the following:

- To outline a procedure and responsibilities of staff working away from the office.
- To highlight relevant legislation applicable to remote working and how to comply.
- To be compliant with the CSU procedure/s on remote working.
- To address the various possible device ownership scenarios: Bring Your Own

Device (BYOD), where staff use personal devices for work. Corporate Owned, Personally Enabled (COPE), where the CCG owns the device but staff are able to use it for personal tasks as well; and Corporate-Only, where the CCG owns the device and limited personal use is allowed.

- To provide guidance for staff and line managers to agree a suitable remote working arrangement, including provision of suitable devices or use of staffs' own devices if appropriate.
- To recommend provision of appropriate devices to staff as they commence employment with the CCG in order to allow remote working from the outset.

All staff are required to comply with the Data Protection Act 1998, Freedom of Information Act 2000, the Computer Misuse Act 1990, and the Common Law Duty of Confidentiality.

3. Definitions

3.1 Remote Working

A working practice which allows an organisation to establish the optimal workforce to support its objectives defined in terms of time (e.g. part time; variable hours), location (e.g. multiple sites; working from home), roles (e.g. multi-skilling) and source (e.g. direct employment or contractors). Remote working is usually supported by technology.

3.2 Device

An electronic information technology or communication device, including but not limited to:

- Desktop PCs,
- Solid state memory cards capable of storing information and being connected to the organisation's computing devices either by themselves or via another device;
- Portable computing and data storage devices which includes but not limited to:
  - Laptops
  - Notebook
  - 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;
  - Smart mobile phones capable of storing more than a basic phone book of contacts;
  - USB Memory or 'Flash' Sticks' and memory cards, capable of storing information;
- 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 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 MAC Address

Media Access Control Address, a unique identifier assigned to a device, used by computer networks to identify and communicate with the device.

3.4 Citrix

Software allowing access to a virtual desktop from a wide range of devices. Provides the user with the experience of using another PC (e.g. an office based PC) from any location.

4. Roles and Responsibilities

4.1 Senior Information Risk Owner

The role of Senior Information Risk Owner (SIRO) is assigned to the Chief Officer. The SIRO takes ownership of the organisation's information risks and act as advocate for information risk to the CCG's Governing Body and Audit Committee by providing written advice on the organisation's information security incident reporting and response arrangements.

4.2 Information Asset Owners

Information Asset Owners (IAOs) are senior members of staff (Directors and Heads of Departments) responsible for providing assurance to the SIRO that information risks within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks. IAOs would have the following responsibilities in respect to mobile working and portable devices:

- Ensure that staff within their team/department/service area are aware of the requirements of this policy.
- Ensure that Data Custodians in their control have identified all potential remote workers within their team/department/service area and have discussed remote working arrangements with them.
- To consider funding for any devices recommended that supports remote working as a result of discussions / agreements between line managers and staff.
- The CSU Information Communication Technology (ICT) helpdesk is informed of any staff, particularly interims, leaving the CCG so that access to systems can be revoked.
- Any devices purchased for staff are returned upon leaving the CCG.

4.3 Data Custodians

An IAO can appoint a Data Custodian to support them in the delivery of their information risk management responsibilities within their team/department/service area. Nominated Data Custodians will ensure that:

- Remote working within their team/department/service area is managed in accordance with this policy.
- Recognise actual or potential remote working/security incidents and take steps to mitigate those risks.
- Report any with remote working/incident to their IAOs and ensure that information their team's asset register is up to date.
- They have discussed remote working with staff and agreed arrangements if applicable.
- Any decisions to support or not support remote working for staff documented and reported to the IAO.

4.4 Remote Workers (Employees)

All Workers (Employees) have the following responsibilities:

- To work in accordance with practice recommended by this policy.
- To comply with legislation and guidance around Information Governance, Data Protection, Health and Safety recommended in this policy.
- To make full and appropriate use of any device provided by the CSU on behalf of the CCG.
- To ensure all mobile devices or items have appropriate encryption active at all times.
- Report any loss or damage to device provided to them.
- To report any technical problems they believe to be associated with remote working immediately to the CSU ICT helpdesk in the first instance and also to their line manager or the Information Governance Manager.
- To report any loss or potential loss to data belonging to the CCG held on their portable devices

4.5 South East Commissioning Support Unit ICT Team

Key responsibilities for the CSU ICT Team include:

- Providing and maintaining access to the CCG network, both directly and via the current remote working platform in line with the current contract/SLA.
- Providing staff with access to the current remote working platform.
- Proving technical support and setup for any device procured by the CCG.
- Providing documented procedures on remote working and use of portable devices.
- Monitoring mobile working activities to ensure compliance with this policy and inappropriate use of the CCG system and assets.

5. Remote Working Practice

5.1 Remote Working

The nature of work for some CCG staff is that team members will visit services in a variety of locations. It is often more efficient for staff to travel direct to location without the need to attend the office beforehand. A staff member's nominated office remains their work base, which means that for the avoidance of doubt they remain primarily an office based employee. Dialogue between staff and line managers should be positive and promote efficient and safe working. It is vital that staff raise work related concerns and work collaboratively to find a reasonable solution.

5.2 Working at Home

Staff can work at home if agreed and authorised by their manager. If staff are unable to attend the office due to reasons beyond their control, i.e disruption to travel, working from home is an acceptable alternative under the CCG's Business Continuity arrangements; however, staff should inform their line managers and other relevant colleagues if they will be working at home. Managers and Directors reserve the right to require a member of staff to attend the office. If staff are unable to honour this request, they may be expected to take a day's annual leave or unpaid leave depending on circumstances.

5.3 Use of Equipment

Staff are expected to take reasonable care of equipment provided to keep risk of theft, data breach and personal safety concerns to a minimum. Equipment should be regularly charged, synchronised and software updated. Any technical issues with the equipment should be reported to the CSU ICT helpdesk and the line manager at the earliest reasonable interval.

5.4 Wireless/ Cordless Computing Connections and Precautions

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 CSU ICT helpdesk and subject to approval, cordless interfaces will only be enabled with organisation's approved protocol settings.

Staff who intend to use portable devices with 'wireless' and other 'cordless' connection interfaces must comply with this policy and other related CCG information security and data protection policies and procedures.

5.5 Direct Connection to NHS Surrey Downs CCG networks

Staff authorised to work from home or from other locations should ensure that they understand CSU ICT remote working procedure/s and access solutions.

All electronic processing devices connecting directly to the CCG'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 staff/user to ensure that device is returned to the CSU ICT helpdesk to enable a manual update of the anti-virus software.

6. Information Security and Confidentiality

All staff should be aware of CCG Information Governance policies relating to the handling of both patient/service-users and corporate confidential information and records. Specific **Do's** and **Don'ts** instructions for this in relation to remote working are below. This instructions should be followed by all staff working for, or on behalf of the CCG away from the organisation premises on an occasional or regular basis (remote or at home).

Staff should also be aware that rights of access by the public to the information held by the CCG under DPA act (1998) and FOI Act (2000) legislation includes information held by staff at home or those working remotely at various destinations.

Do's:

- Remember that as all work-related documents are the organisation's assets, and as such fall within the scope of FOI and DPA
- Work directly from the organisation's server and save documents on the CCG network drives via CITRIX or via a CCG issued encrypted USB data stick.
- Where data is stored on the CCG issued memory sticks, it should be transferred to the shared drives at the earliest available opportunity.
- Take copies of paper files or electronic documents home, rather than originals, unless there is no alternative and only if necessary. The 'original' or 'master' copy of the information should be stored at the CCG and not at home,
- Print only the minimum required to undertake work activity.
- Make use of security features such as encryption and password protection. Encryption of the device or medium is mandatory if it includes corporate or personal confidential data relating the to operations or business of the CCG
- If you receive work email on your mobile device, ensure the phone AND any storage is encrypted and ensure the security functions (PIN code to unlock etc) are engaged
- Take all reasonable steps to maintain security of and prevent loss or damage to any data and/or records taken away from the Organisation.
- Take reasonable measures to protect work related information at home from unauthorised access, amendment or loss (This includes access by family members).
- Consider what practical measures are needed to ensure the home environment is secure, i.e. not leaving papers in household areas where disclosures can take place.
- Take precautions against theft and loss, particularly on the journeys to and from work.
- Use CCG and/orNHS.net e-mail accounts for work and personal email accounts for personal use only – avoid mixing the two.
- Keep home computer systems and applications virus protected and up-to-date.
- Dispose of all confidential papers files in the CCG confidential bins at CCG premises only.

- Keep paper records separate from equipment and technology (because of the risk of theft) they must be carried in separate bags.
- Assess the risk involved with the loss of personal and business sensitive data, by addressing the following questions:
  - How serious would the consequences be if someone gained unauthorised access to this information?
  - How likely it is that someone could gain access to this information?
  - What security procedures and measures are in place and are they appropriate?
  - What is the cost of implementing appropriate security procedures and measures?
- Any person confidential data or corporate confidential data transferred to an encrypted USB data stick must:
  - be a copy of what is on your secure network drive;
  - remain encrypted and must not be transferred to any other external system, e.g. a home or other computer;
  - be worked on by opening and saving changes back to the USB data stick;
  - be returned to the appropriate location, as an updated version of the file/s on your organisation network drive and deleted from the memory stick after the work required is completed.

Don’ts:

- Use your home computer to store organisation information.
- Use ‘cloud’ storage systems such as Drop Box, Microsoft One Drive, or Google Docs
- Remove paper confidential files from the CCG premises unless it can be stored securely.
- Leave paper or electronic files where they could be accidentally viewed by others, including family members.
- Use a personal e-mail account for CCG’s business or vice-versa. If you have to use your work email account for personal business please keep separately and store separately to avoid possible problems with DPA or FOI requests.
- Leave CCG information data or electronic media in unattended vehicles, even if locked in the boot.

7. Use, Support and Provision of Devices

7.1 Bring Your Own Device (BYOD)

In some circumstance the CCG allows staff to use their own portable devices smartphone for work. The CCG is not able to contribute financially to the purchase or lease of devices; however, an appropriate level of technical support will be provided, as detailed in the section below. As neither the CSU ICT nor manages or maintains these devices, it’s critical that staff follow the guidelines in this document.

As device owners, staff are requested to:

- Settle any service or billing problems with the carrier (the network).
- Keep the device current by installing software updates/patches when they become available.
- Install any software that your manager agrees is required for business use.
- Keep any relevant warranty information.
- Replace the battery if and when required.
- Perform all data, settings, media and application backups.
- Inform the CSU ICT helpdesk and your line manager immediately if your own device is lost/stolen (if you use it for work related purposes).
- Ensure that you apply all security measures such as PIN code/locked screen access control, as well as encryption of the device AND any data cards in the device. **Encryption of the device is essential and mandated if it includes any corporate or personal confidential data**
- It is your responsibility to make sure you know how to **wipe/delete** data from your own device if it is lost/stolen so that work related information is not at risk of being in the public; where appropriate the CCG will provide guidance on this.

7.2 Corporate Owned, Personally Enabled (COPE)

Corporate Owned, Personal Enabled (COPE) devices are managed by the CSU ICT department/directorate; this includes portable devices listed on section 3.2 of this Policy. Users of COPE devices are responsible for:

- Installing/agreeing to software updates that are made available by the ICT helpdesk.
- Reporting a lost or stolen device immediately.

Corporate Only

Desktop PCs, including those provided on hot desks and in meeting rooms, and laptops provided for the purposes of delivering presentations should be considered as Corporate Only devices. Users of Corporate Only Devices are responsible for:

- Installing/agreeing to software updates that are made available by the CSU ICT helpdesk.
- Reporting a lost or stolen device immediately.

8. ICT Support

The ICT helpdesk is responsible for configuring and providing technical support to all devices COPE and Corporate Only devices. Staff can expect a COPE or Corporate Only device to be supplied with all relevant applications installed locally and fully configured to allow them to connect to wireless and mobile (if enabled) networks and access e-mail, calendar and contact services remotely.

For BYOD devices, the CSU ICT helpdesk will:

- Ensure that devices are compatible with software required to access the CCG network.
- Set up to access approved applications and networks.
- Configure access to the email, calendar and contact service.
- Configure Wi-Fi access.

8.1 Supported Devices

The following devices / operating systems are currently supported (i.e. are able to run Citrix software):

Notebooks / Desktop PCs	Smart Phones	Tablets
Apple Mac OS (iMac, Mac Pro, Macbook, Macbook Pro, Macbook Air)	Apple iOS (iPhone 4, 4s, 5, 5c, 5s, 6, 6 Plus)	Apple iOS (all iPads including iPad Air, iPad Air 2 and iPad Mini)
Microsoft Windows XP, Windows 7, Windows 8, Windows 8.1 (Most models including Dell, HP, Lenovo	Windows (Nokia Lumia – all models)	Windows 8 / 8.1 / RT (Microsoft Surface, Dell Venue Pro, Nokia Lumia
	BlackBerry & BlackBerry 10 (BlackBerry Bold, Curve, Q5, Q10, Z30, 9720)	BlackBerry Playbook
	Android (Alcatel, Doro, HTC, Huawei, LG, Motorola, Samsung, Sony)	Android (Samsung Galaxy, Google Nexus, Kindle Fire, Acer Iconia, Sony Xperia)

This list is not exhaustive and may change as technology develops.

9. Mandatory IG training for all staff

The CCG recognise the importance of an effective training structure and programme to deliver compliant awareness of IG and its integration into the day-to-day work and procedures.

All permanent/temporary/contract staff including lay members will complete mandatory training modules commensurate with their level of access to personal confidential data within the first week of employment, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles.

10. Monitoring & Compliance

Compliance with this policy will be audited with reference to records of decisions about remote working and portable devices maintained by IAOs and Data Custodians within their department/service areas.

Devices may be interrogated to provide information on how frequently and for what purpose they are being used.

The effectiveness of this Policy will be measured in terms of improvements in productivity and wellbeing as reported by staff and managers or by savings in terms of resources (e.g. paper, toner, desk availability).

Additionally, remote workers may be surveyed periodically to give their views on working arrangements. This may be done as part of routine annual appraisals, the CCG staff survey or by means of a separate survey.

11. Dissemination and Implementation

This Policy will be publicised in line with the framework for the development and management policy and procedural documents. The policy will be available on the CCG website. Any future amendments/revisions will be brought to the attention of staff via internal communications. Managers will arrange for this policy and any subsequent amendments to be brought to the attention of all staff and ensure that it is accessible to them.

12. Related Documents

The following documentation relates to the security of information and together underpins the CCG's Information Governance Framework. Technical information security issues, operational and strategic authority rests with the South East CSU ICT Team. This Policy should be read in conjunction with other information documents, including, but not limited to:

- Information Security Policy
- SE CSU Remote Working Procedure
- South East CSU Bring Your Own Device (BYOD) Policy
- Confidentiality Policy - Data Protection
- Information Governance Framework
- Freedom of Information Policy
- Information Security Policy
- IG and Cyber Security Incident Management and Reporting Procedure