Working with you to make Sheffield HEALTHIER

NHS Sheffield Clinical Commissioning Group

Remote Working and Portable Device Security Policy

August 2019

Version:	5.0
Policy Number:	CO18/08/2020
Date ratified:	27 August 2019
Name of originator/author:	Deputy Director of Commissioning and Performance
Name of Sponsor:	Director of Commissioning and Performance
Name of responsible committee	Governance Sub Committee
Date issued:	September 2019
Review date:	August 2020
Target audience:	All staff

To ensure you have the most current version of this policy please access via the NHS Sheffield CCG Intranet Site by following the link below:

http://www.intranet.sheffieldccg.nhs.uk/policies-procedure-forms-templates.htm

MINDFUL EMPLOYER

disability confident EMPLOYER

Policy Audit Tool

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Please give status of Policy: Revised

1.	**Details of Policy/Procedural Document**	
1.1	Policy Number:	CO18/08/2020
1.2	Title of Policy/document:	Remote working & portable device security policy
1.3	Sponsor	Director of Commissioning & Performance
1.4	Author:	Deputy Director of Commissioning & Performance
1.5	Lead Committee	Governance Sub-Committee
1.5	Reason for policy/document:	To promote safe and secure access to SCCGs information and IT resources from remote locations, whilst protecting SCCG and staff members from the risks arising from enabling such access. This is in line with the requirements as detailed within the Data Protection Act 2018, General Data Protection Regulation 2018. This policy also ensures that behaviours and processes within SCCG are aligned with all legal obligations.
1.6	Who does the policy affect?	All staff
1.7	Are the National Guidelines/Codes of Practice etc issued?	Yes
1.8	Has an Equality Impact Assessment been carried out?	Yes
2.	**Information Collation**	
2.1	Where was Policy information obtained from?	Previous Policy, NHS Mail terms and conditions as produced by NHS Digital and Information Governance expertise.
3.	**Policy Management**	
3.1	Is there a requirement for a new or revised management structure for the implementation of the Policy?	No
3.2	If YES attach a copy to this form.	
3.3	If NO explain why.	Existing policy
4.	**Consultation Process**	
4.1	Was there external/internal consultation?	Internal
4.2	List groups/persons involved	SCCG Staff Forum, Directorate teams, JSCF, IG Group, EMBED IG Team
4.3	Have external/internal comments been included?	Yes
4.4	If external/internal comments have not been included, state why.	
5.	**Implementation**	
5.1	How and to whom will the policy be distributed?	All SCCG Staff

5.2	If there are implementation requirements such as training please detail.	
5.3	What is the cost of implementation and how will this be funded	
6.	**Monitoring**	
6.1	How will this be monitored	Number of adverse incidents reported Number of complaints received
6.2	Frequency of Monitoring	Monthly

Version Control

VERSION CONTROL				
Version	**Date**	**Author**	**Status**	**Comment**
1.0	July 2014	Information Governance Group		
2.0	July 2016	EMBED IG Team	Review	
3.0	April 2019	EMBED IG Team / Deputy SIRO	Review	Incorporated NHS Mail terms and conditions and Mobile Configuration Guide
4.0	June 2019	Deputy SIRO	Review	Incorporated suggested comments following internal engagement through staff forum and JSCF
5.0	August 2019	Deputy SIRO	Review	Incorporated suggested comments following virtual sign off by Governance Sub Committee members prior to formal ratification

Contents

1 Introduction & Purpose

1.1 NHS Sheffield Clinical Commissioning Group (SCCG) requires that staff are able to fulfil their roles effectively, and to this end aims to provide technical solutions which allow staff and other authorised people to access SCCG's IT resources in a secure and flexible manner from sites other than SCCG offices.

1.2 In addition to this, due to consumer electronic devices such as smart phones and tablet computers seeing a huge rise in popularity, available features and capability means that staff members may wish to use these devices in the workplace to carry out their role. This may also mean that individuals may wish to use their own personal device to access and store corporate information (some of which will be sensitive and may be classified as personal data as defined by the Data Protection Act 2018) as well as their own. This is defined within this policy as 'bring your own device' BYOD.

1.3 What is Remote Access? Remote Access refers to any technology that allows you access to the organisation's IT systems from other, different locations. This is typically via other organisations' networks; public WiFi; home broadband or mobile phone networks; as well as through the GovRoam WiFi service.

1.4 What is a Portable Device? A portable device is generic term used to describe any computing device that is designed to be used in more than one location, such as laptops, tablet computers (e.g. iPads), smartphones and USB flash drives.

1.5 The purpose of this policy is to promote safe and secure access to SCCG's information and IT resources from remote locations, whilst protecting SCCG and staff members from the risks arising from enabling such access. This is in line with the requirements as detailed within the Data Protection Act 2018 and General Data Protection Regulation 2018. This policy also ensures that behaviours and processes within SCCG are aligned with all legal obligations.

2 Scope

2.1 This policy applies to:

- All staff, including Governing Body members, who are expected to comply with this policy when using SCCGs systems remotely, or using portable devices with SCCG's IT infrastructure. This includes the remote access of NHS mail in which the content of the emails relate to the work being undertaken for SCCG.

- Employees of other organisations, contractors, students, volunteers and other individuals, who have been granted permission to use SCCG's remote access facilities or portable devices, are also expected to comply with this and other relevant policies.

2.2 Failure to comply with this policy may result in disciplinary action, your association with SCCG being terminated and remote access rights being revoked. It may also bring into question any professional registration as well as personal liability if patient sensitive information is accessed or shared for non-work related purposes as per the Data Protection Act 2018.

2.3 This policy is to be read and used alongside other related policies such as: Information Governance Framework, Email Policy, Internet Acceptable Use Policy and the Mobile Telephone Policy & Procedure.

3 Definitions

SCCG	Sheffield Clinical Commissioning Group
GDPR	General Data Protection Regulation 2018
IT	Information Technology
IG	Information Governance
NHS	National Health Service
BYOD	Bring Your Own Device

4 Roles & Responsibilities

4.1 SCCG Staff

- It is an individual decision for any staff member to decide to use a personal device for work related purposes. Under no circumstances is it expected that a staff member will automatically use their own personal device, and this will not be enforced.
- Despite personal ownership of a device, the organisation expects the user to assume certain responsibilities if a staff member makes the decision to use such a device to access SCCG information or connects to SCCG's resources. Staff members must ensure that they comply with all sections of this policy.
- If accessing NHS Mail from a personal device, the staff member would automatically accept the terms and conditions of NHS Digital who manage NHS Mail, which is external to SCCG. This policy mirrors such terms and conditions and draws particular attention to the device configuration and management guide. The link to the NHS Mail terms and conditions is detailed in Appendix 1 and the link to the device configuration guide is detailed in Appendix 2, however the following are pertinent points that require emphasis within this policy:

  Terms and Conditions:

  - Section 2.2: The NHS Mail services have been provided to aid the provision of health and social care and this should be your main use of the service.

  - Section 3.1.10: If you are accessing your NHS Mail account from a non-corporate device i.e. a home computer, personally owned laptop or in an internet café, you should only access the service via the web at www.nhs.net and not through an email programme such as Microsoft Outlook or Exchange, unless you have explicit permission from your own organisation to do so.

  - Section 4.3.8: If it is likely you may be sent personal and/or sensitive information you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.

Mobile Configuration Guide for NHS Mail:

- Key Features: Security features are automatically applied to devices that are able to support security policies, e.g. an automatic screen lock after the device has been inactive for a maximum of 20 minutes; self-service device password reset and remote wipe facility if the handset is lost or stolen.
- Key Features: The service is available on different devices including Windows Mobile, Nokia, Blackberry, Android, Apple IPhone and IPad.
- Key Features: Devices that have been modified by techniques such as 'Jailbreaking' or 'Rooting' (which refers to allowing someone to gain full access to the devices' operating system and therefore all apps and features held within it) must never be connected to NHS Mail as the security/integrity of the device cannot be guaranteed. Devices should be kept up to date with the latest software available via the manufacturer.
- Mobile Device Configuration: Only devices which support the Exchange Active Sync protocol (please refer to Appendix 2) and have inbuilt encryption at rest capability should be connected to NHS Mail.
- Protecting a Mobile Device: If you have a mobile device set up to access NHS Mail, you may notice a range of security features automatically applied to it. This is to minimise the risk of data loss. Security features include:

    - An encrypted connection between the mobile device and the NHS mail service.
    - Implementation of a password to access the mobile device.
    - A limit on the size of email attachments that can be downloaded – by default 10MB.
    - A remote-wipe facility, meaning that the data held on the mobile device can be deleted if it is lost or stolen.
    - In addition, some mobile devices automatically encrypt the data they contain 'at rest', in other words the data held on the phone is encrypted and can only be read after the phone is unlocked by the user, preventing access should it be lost or stolen. Encryption at rest is automatically enabled on connection to NHS Mail on those devices that support this feature. It is important that sensitive or patient identifiable data isn't held on mobile devices that do not have built-in encryption at rest capability or those where encryption at rest cannot be remotely enabled. It is a mandatory Department of Health requirement that only encrypted devices carry such data.

- It is therefore the responsibility of SCCG staff to inform their line manager if they will be using their own personal device to access NHS Mail so this can be logged and managed if the device is lost or stolen.
- In the event of a personal device being lost or stolen, the staff member should as soon as possible, securely log on to NHS mail and wipe the device. The staff member should also log the incident on Datix and inform a member of the Information Governance Team in order to ensure the device has been remotely

wiped in accordance with this policy. If a personal device is sold or no longer being used, then the device will be wiped of any work related information and emails.

- It remains the staff member's responsibility to adhere to the NHS Mail terms and conditions and Mobile Configuration guide when handling patient sensitive information. SCCG will not be held responsible if the misuse and handling of information occurs. Under the Data Protection Act 2018 and General Data Protection Regulation 2018, the consequence of such behaviour and actions remains with the individual and SCCG will follow the guidance as provided by the Information Commissioners Office (ICO).
- Only those members of staff with remote access permission to SCCG's network can access the network remotely using appropriate equipment. If a staff member requires to work remotely in order to carry out their role, this will be made available in accordance with the Mobile Telephone Policy and Procedures and following discussion with their line manager.
- No member of staff will use USB sticks that are not encrypted or meet the security standards of SCCG. Installed security software on SCCG computers and laptops automatically reject any USB sticks that do not meet the security criteria. If a staff member requires the use of a USB stick, this will be made available via a discussion with their line manager.

4.2 Line Managers

- All line managers will agree to the use of a personal device being used for work purposes as per this policy and associated policies by their staff
- All staff members who wish to use a personal device will inform their line manager, who is responsible for keeping a log of the staff members as well as the type of device, which will be given to the Information Governance Team
- Ensure that all staff members have read and understand this policy and associated policies and that they agree to adhere to it
- For those staff members who require the use of a device to access SCCG related information in order to carry out their duties but do not wish to use their personal device, then the Mobile Telephone Policy and Procedures should be referred to

4.3 Information Governance Team

- The Information Governance (IG) Team is responsible for overseeing the implementation of the Remote Working and Portable Device Security Policy including monitoring compliance. This will include holding details of the staff members including device details who access SCCG information through NHS Mail or other IT resources
- The IG Team will receive a monthly report of users and their devices from NHS Digital to ensure that all devices meet the required standards and therefore uphold all of the required security protocols
- The IG Team will follow the policy by ensuring that the staff member has successfully wiped a device if lost or stolen in accordance with this policy

4.4 SCCG specific responsibilities and rights

Access to and use of remote devices

SCCG will:

- Ensure that all staff members who require access to remote devices in order to carry out their role will be given sufficient equipment. This could be with regards to items such as a laptop, remote access token such as PinSafe or a mobile telephone. This will be in accordance to the SCCG's Mobile Telephone Policy and Procedures
- Not assume or expect a staff member to use a personally owned piece of equipment to carry out their role

4.5 Trade Union Representatives specific responsibilities and rights

- Ensure they are familiar with the policy and procedure.
- Advise and represent employees who are members of a recognised Trade Union

5 Monitoring effectiveness of the policy/procedural document

- All email used on local NHS systems is monitored for viruses, malware and spam
- All email (incoming and outgoing) on local NHS systems is logged automatically
- Monitoring logs are audited periodically
- The use of email is not private. The content of email is not routinely monitored but SCCG reserves the right to access, read, print or delete emails at any time whilst also following due governance processes and procedures
- Any monitoring or interception of communications will be carried out in accordance with legislation such as the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 2018, the General Data Protection Regulation, the Human Rights Act 1998 and specific procedures around monitoring and privacy

6 Review

6.1 Investigating breaches of this policy

This document may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed after twelve months and thereafter on a bi-annual basis or when a change in legislation dictates.

SCCG will:

- Investigate breaches of this policy, actual or suspected, in accordance with SCCG procedures.
- Where appropriate, invoke the SCCG's disciplinary procedure for breaches of this and the Fraud, Bribery and Corruption Policy.
- Where appropriate, make a complaint to an individual's employing organisation and co-operate fully into any investigation of that complaint where breaches of this policy are committed by users who are not employees of SCCG (such as staff on secondment to SCCG, Honorary Contract holders and users given access to systems by agreement between SCCG and the user's employing organisation).
- Where appropriate take legal action (that is, criminal or civil proceedings) in respect of this policy.

6.2 Liability

- SCCG will not be liable for any financial or material loss to an individual when using their own personal equipment to access work email or information.

7 References and links to other documents

- All staff are expected to comply with this policy as well as the NHS Email policy and guidance published on the NHS Mail portal, https://portal.nhs.net/Help/policyandguidance
- **In particular the NHSMail Acceptable Use Policy (AUP) which covers the use of NHSMail Email and Skype for Business instant messaging must be adhered to**
- This policy is based on current law, NHS Information Governance standards and accepted standards of good practice; your duty to handle SCCG corporate and person confidential information appropriately arises out of common law, legal obligations, staff employment contracts and professional obligations.[1]
- Any breaches of this policy will be fully investigated in accordance with SCCG processes which may result in disciplinary action, referral to the Local Counter Fraud Specialist for further investigation and, if appropriate, your employment or association with SCCG being terminated. It may also bring into question your professional registration and may result in disciplinary, civil or criminal proceedings
- If there is anything that isn't clear or which you do not understand in this policy you must contact your line manager, in the first instance, or the Information Governance Lead for further information.
- Please note that the procedures and policies outlined in this policy and any related policy may be changed at any time. You will be alerted to this via established SCCG communication routes.

[1] For example, with the General Medical Council, Nursing and Midwifery Council or Health Professions Council

8 Equality & Diversity Statement

NHS Sheffield 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.

NHS Sheffield CCG embraces the six staff pledges in the NHS Constitution. This policy is consistent with these pledges.

9 Disability Confident

NHS Sheffield CCG has been accredited with the Disability Confident Award – level 1. This is in recognition of meeting the commitments regarding employment of disabled people and permits the organisation to use the Disability Confident logo on all of its stationery. The Disability Confident symbol should be added as a footer to all policies / procedural documents.

NHS Sheffield Clinical Commissioning Group

NHS Sheffield CCG Equality Impact Assessment 2016

Equality Impact Assessment

Title of policy or service:	Remote Working & Portable Device Security Policy	
Name and role of officer/s completing the assessment:	Sandie Buchan, Deputy Director of Commissioning & Performance (Sheffield CCG) Gershon Nubour, Information Governance Manager (eMBED)	
Date of assessment:	7th May 2019	
Type of EIA completed:	**Initial EIA 'Screening'** ✓ ***or*** **'Full' EIA process**	

1. Outline	
Give a brief summary of your policy or service • Aims • Objectives • Links to other policies, including partners, national or regional	To promote safe and secure access to SCCGs information and IT resources from remote locations, whilst protecting SCCG and staff members from the risks arising from enabling such access. This is in line with the requirements as detailed within the Data Protection Act 2018 General Data Protection Regulation 2018. This policy also ensures that behaviours and processes within SCCG are aligned with all legal obligations. This policy is to be read and used alongside other related policies such as: Information Governance Framework, Email Policy, Internet Acceptable Use Policy and the Mobile Telephone Policy.

Identifying impact:

- **Positive Impact:** will actively promote or improve equality of opportunity;
- **Neutral Impact:** where there are no notable consequences for any group;

- **Negative Impact:** negative or adverse impact causes disadvantage or exclusion. If such an impact is identified, the EIA should ensure, that as far as possible, it is justified, eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information
This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.

	What key impact have you identified?			For impact identified (either positive an or negative) give details below:	
(Please complete each area)	**Positive Impact**	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	☐	x	☐		
Age	☐	x	☐		
Carers	☐	x	☐		
Disability	☐	x	☐		
Sex	☐	x	☐		
Race	☐	x	☐		
Religion or belief	☐	x	☐		
Sexual orientation	☐	x	☐		
Gender reassignment	☐	x	☐		
Pregnancy and maternity	☐	x	☐		
Marriage and civil partnership (only eliminating discrimination)	☐	x	☐		
Other relevant groups	☐	x	☐		
HR Policies only: Part or Fixed term staff	☐		☐		

IMPORTANT NOTE: *If any of the above results in '**negative'** impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.*

Having detailed the actions you need to take please transfer them to onto the action plan below.

3. Action plan				
Issues/impact identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication				
When will the proposal be reviewed and by whom?	**Lead / Reviewing Officer:**	**Information Governance Manager (eMBED)** **Information Governance Group (Sheffield CCG)**	**Date of next Review:**	**August 2020**

Appendix 1:

NHS Mail usage terms and conditions

https://portal.nhs.net/Home/AcceptablePolicy

Appendix 2:

NHS Mail mobile configuration guide

https://support.nhs.net/knowledge-base/mobile-configuration/