NHS
Buckinghamshire
Clinical Commissioning Group

Mobile Devices and Remote Working Policy v1.4

CONTENTS

NHS
Buckinghamshire
Clinical Commissioning Group

1. Policy Statement

This policy sets out the responsibilities of staff in regards to the use of mobile technology wherever they are working, which includes off-site/ remote working.

This policy has been developed to ensure all staff who have a requirement to access the organisation's systems remotely or to use mobile devices, do so securely and without introducing unacceptable risks to both the processing of data and the network.

Remote access is a method of accessing files and systems remotely via an authorised Virtual Private Network (VPN) token.

Due to significant changes to working practice and the development of technology, remote access to systems by NHS staff is now seen as the normal way of working.

Personal devices are not permitted to be used for work purposes other than expressly permitted by the Data Controller, whilst ensuring that the device is encrypted.

This policy applies to all staff who work at the organisation with legitimate right to access the systems, e.g. contractors and temporary workers. This policy is also to be read in conjunction with an equivalent policy from NHS South, Central and West Commissioning Support Unit as supplier of the CCG's hardware and software infrastructure.

2. Principles

Critical business processes rely on easy and reliable access to organisational information systems. Business needs to be conducted remotely with confidence and confidentiality, especially when dealing with sensitive information. This document sets out the policy for holding, recording, storage, sharing and using information via mobile devices (laptop, smart phone etc) and includes a set of controls that can be applied to reduce risks associated with remote access and agile working.

At all times the processing of information must be in accordance with national guidance including Department of Health Codes of Practice ISO 27001: 2013 – Information Security, Data Protection Act (2018), GDPR (2018), Caldicott Principles and any local organisational policies.

Failure by any member of staff of the organisation to adhere to this policy will be viewed as a serious matter and may result in disciplinary action.

3. Definitions

User Within this policy, the term 'user' includes anyone who uses the organisations' network, phone or computing facilities to access the network, including but not exclusively:

Employees, Governing Body Members, Lay Members, Bank Workers, volunteers, honorary contractors, secondees or other authorised users working for or on behalf of the organisation.

Mobile devices – This includes but is not limited to laptops, notebooks, iPads, tablets, smart phones and external CCG encrypted storage devices.

4. Scope of Policy

Ensure the appropriate use of mobile devices including laptops, notebooks, iPads, tablets and smart phones.

Ensure that access to information is conducted in a secure and confidential environment regardless of location.

Applicable legislation and Freedom of Information principles apply to remote workers operating CCG approved mobile devices to process NHS information.

5. Criteria for the issuing of mobile devices

Users will be eligible to have a mobile device if it is deemed necessary to their role. Laptops are issued as standard to CCG employees. Should users require laptops to a specification other than the standard, or have a need for a mobile phone or other mobile device, requests should go through the CCG Senior Management Team for approval.

On receipt of a mobile device, a mobile devices declaration form must be completed and given to the internal CCG Mobile Devices Lead.

6. Replacement mobile devices

The CCG expects all users who have been allocated mobile devices to take the utmost care and responsibility for them. If a device is lost or stolen, it should be reported immediately to the CCG Mobile Devices Lead or deputy, as well as their line manager. Where appropriate, a police report should also be filed in order to receive a crime reference number.

If a device is broken or faulty, please report this to the CCG Mobile Devices Lead or deputy and notify your line manager. A temporary device may be issued if one is available until the device is repaired. If the device cannot be repaired, a replacement device will be sourced through the CCG Mobile Devices Lead.

NHS
Buckinghamshire
Clinical Commissioning Group

7. Change of User including termination of contract

On termination of contract, the user must return their device to Internal Mobile Devices Lead and must complete the CCG's '

All accessories eg charger, power cable, data cable, bag or other item supplied by the organisation for use with the mobile device must also be returned

In line with the user's signed paperwork on receipt of the mobile device, when returning the device(s), if there is any damaged or missing equipment preventing re-issuing of the devices, the user may be personally charged where appropriate.

It will be the responsibility of the manager to ensure the relevant paperwork is completed and items returned.

Mobile devices issued to an individual must not be passed to another user all device reassignments must go through the CCG Mobile Devices Lead. This is to ensure the correct mobile device receipt declarations are completed and that the asset register remains up to date.

If staff are transferred to a new role, a new request will need to be submitted to the CCG IT Lead to ensure the new role requires the same level of equipment. If devices are not required for the new role, equipment must be returned in the usual way.

On return of a mobile device, the user will ensure all data has been deleted before returning the item to their line manager.

8. Conditions of use

Where individuals are using a CCG smart phone for emails or internet usage, it should be made in the most cost effective manner, using Wi-Fi wherever possible to minimise costs. Work related calls to UK mobiles and landlines are included within the contract, with no additional cost to the organisation. Contacting Overseas and 0800 numbers are not included in the mobile phone allowance, so where possible, an appropriate alternative method such as Mitel or Skype should be sought.

Conference calls should also be conducted over Wi-Fi wherever possible to keep the cost to a minimum.

Confidential information must not be discussed in open or inappropriate areas.

Users must not use their mobile phone while driving, even with a hands free kit.

NHS
Buckinghamshire
Clinical Commissioning Group

9. Appropriate use of mobile devices

Unauthorised software must not be installed on any organisational equipment, including mobile devices. Personal confidential information must not be sent via email unless it complies with the GDPR Data Protection Act 2018.

Mobile devices must have security options enabled such as PIN or password protection and minimum software requirements as deemed appropriate for the device. No personal device should be connected to the CCG network at any time.

All mobile phones (IPhone only) are unlinked on return from personal iTunes accounts and staff are asked to wipe any personal information from these devices prior to return.

9a Permission authorised by the CCG (as Data Controller)

NHSMail
The Mobile Configuration Guide for NHSmail issued by NHS Digital, states that should an individual wish to access NHSmail using a personal device, they are required to obtain approval from their own organisation to ensure compliance with local information governance policies.

This policy documents that this approval is granted without further approval required, on the basis that NHSMail as a tool in itself has appropriate data security and protection measures and that no data, personal or otherwise, is captured and stored on local devices where the NHSMail web app is used.

MS Teams
This policy also confirms that no additional approval is required for MS teams for the same reason as above in respect of NHSMail.

Authority for use on a personal device of any tool other than the above must be sought in the first instance from the CCG Data Protection Officer, with any Data Protection Impact Assessment undertaken as may be deemed necessary. This shall include need for secure login arrangements as appropriate through NHS SCWCSU service desk. This shall also include arrangements for backup of data and wipe of data in the event of theft/loss, which is otherwise largely irrelevant for personal devices.

In any event, the type of information or services that can be accessed or stored on personal mobile devices shall not include any storage of patient identifiable or confidential data. The same shall apply to access controls and software versions which will likely vary according to the device proposed to be used.

10. Responsibilities

All users with remote access and/or use of a mobile device are responsible for complying with this policy and associated standards. All staff must safeguard organisational equipment and information resources, and notify the organisation immediately of any security incidents or breaches.

All users of information systems, devices and applications via the network must ensure they are aware of and comply with their security responsibilities. Irresponsible or improper actions will result in disciplinary action. Appropriate risk assessment between employee and line manager will be undertaken prior to any remote working arrangements being agreed.

11. Health and Safety

The management of Health and Safety at Work Regulations 1999 require the CCG to ensure all information and instruction is provided to conform to the appropriate Health and Safety Legislation and associated Regulations. Since December 2003, it has been an offence to use a hand held device whilst driving. It is the responsibility of the staff member not to use a hand held device whilst driving. If a member of staff uses a hand held device whilst driving there is a risk of prosecution and penalty charge, the CCG are not responsible for any penalty charge or other liability.

Using a hands free kit can also result in a fine and penalty points, under existing Legislation for failing to have proper control of the vehicle if the driver is distracted or a risk of prosecution for careless or dangerous driving.

When on CCG business, staff must not use a mobile device within their car, if you need to make/take a call, pull over and park in a safe place and switch off the engine.

Users must not use their mobile phone while driving, even with a hands free kit.

If for any reason, a device becomes damaged in a way which could affect the health and safety of the user (such as a smashed screen), refer to section 6 of this policy.

Reasonable costs for screen savers or protective cases can be claimed via e-expenses to protect mobile devices.

12. Security

The user must take all possible precautions to ensure the security of CCG mobile devices is maintained at all times. Devices should be password enabled and encrypted at all times. Mobile devices are frequently stolen – to reduce the risk of this, mobile devices should never be left unattended, and this includes leaving devices locked in an unattended vehicle.

All security incidents and weaknesses must be reported to your line manager and recorded on Datix.

13. Private access

Mobile devices issued by the CCG should only be used for CCG business. The CCG receives itemised bills and data usage and monitors this regularly. Any unusually high usage will be referred to the line manager for review. It is the individual's responsibility to respond to any discrepancies.

Staff provided with a mobile phone may receive bills for personal usage.

NHS
Buckinghamshire
Clinical Commissioning Group

14. Equality Impact Assessment

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

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• 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	If an employee with a disability is issued with a mobile device, a discussion with the employee should take place to discuss any reasonable adjustments that may be required. HR to support.
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	None	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	None	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	None	

This policy has been subject to an equality impact assessment. If you have identified a potential discriminatory impact of this procedural document, please refer it to Julie Goddard, together with any suggestions as to the action required to avoid/reduce this impact.

NHS
Buckinghamshire
Clinical Commissioning Group

For advice in respect of answering the above questions, please contact Julie Goddard Julie.goddard3@nhs.net

15. Review period

The policy and procedure will be reviewed periodically by ConsultHR, in conjunction with operational managers and trade union representatives. Where review is necessary due to legislative change, this will happen immediately.

Document Control Summary

Title	Mobile Devices and Remote Working Policy
Lead Officer	Julie Goddard
Purpose of document	To state the CCGs policy in relation to Mobile Devices to be disseminated to all staff.
Status	Final
Version No.	1.4
Date	November 2020
Author(s)	HR Manager, SCWCSU
Date of approval by Staff Partner Forum	3 November 2020
Review Date	Three Years or sooner if required
Groups/individuals overseeing development and approval	Staff Partnership Forum
Publication	Intranet: Yes (ConsultHR) CCG

Version Control Summary

Date & Version	Author/Editor	Comment
January 2019 v1.3	Julie Goddard SCWCSU HR Manager	Review at Staff Partnership Forum July 2019 Agreed July 2019
November 2020 v1.4	Russell Carpenter, Head of Governance/Board Secretary	Data Protection Act updated to refer to 2018 not 1998.Updates arising from management actions within a Secure Remote Working, Information Security and Operational Resilience internal audit by RSM. Section 1: *This policy is also to be read in conjunction with an equivalent policy from NHS South, central and West Commissioning Support Unit as supplier of the CCG's hardware and software infrastructure.* Section 9: Insert of details on: minimum software requirements for personal devices and permission authorised by the CCG (as Data Controller). Section 10: Appropriate risk assessment between employee and line manager will be undertaken prior to any remote working arrangements being agreed.