Mobile Working Policy and Guidelines

May 2020

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.

Name of Policy:	Mobile Working Policy and Guidelines
Date Issued:	July 2020
Date to be reviewed:	2 years after approval

Policy Title:	Mobile Working Policy and Guidelines v2.0	
Supersedes: (Please List)	Mobile Working Policy and Guidelines V1.1	
Description of Amendment(s):	Minor changes to legislation. Removal of eMBED Spelling and Grammar.	
This policy will impact on:	All Staff , temporary staff, seconded staff	
Policy Area:	IT and Data Protection	
Version No:	2.0	
Author:	Humber IG Team	
Effective Date:	July 2020	
Review Date:	May 2022	
Equality Impact Assessment Date:	14/04/2020	
APPROVAL RECORD		**Date:**
	IAGC	07/07/20
Consultation:	Hull CCG Deputy Heads	05/02/20
	Information Governance Steering Group	05/02/20

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on website
0.1	C Wallace	Document created		
1	C Wallace	Reviewed as part of lifecycle. No changes required submitted for extension.	8 March 2016	
1.1	M Culling	Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2018 incorporating the requirements of the General Data Protection Regulation).	IAGC 16 January 2018	January 2018
2.0	H. Gillingwater	Minor changes to legislation. Removal of eMBED Spelling and Grammar. Additions for Home Workers Alternative Communication tools SAR/ FOI Requests	IAGC 07 July 2020	July 2020

CONTENTS

1. INTRODUCTION

Mobile working allows Hull Clinical Commissioning Group (CCG) to make cost savings while ensuring that staff remain interconnected and able to work from almost anywhere.
The CCG has different types of workers falling into one of the following categories:-

Fixed
Fixed workers will:

- Spend most of their time working at one fixed site.
- May have specific, individual equipment / furniture needs to be able to perform their role and work effectively
- Seldom away from their desk except for meetings with colleagues in the office
- Do not need to work from non-CCG sites.

Equipment

- Use of Fixed Phone on Desk or mobile phone.
- Use of laptop which can sit in a docking station on the desk.

Flexible
Flexible workers will:

- Have the ability to effectively deliver their work utilising space across a range of CCG buildings or locations where wifi is available
- May also spend time attending meetings or working at other NHS, Trust, partner, or client sites
- Spend a large percentage of their time attending meetings/other similar events and/or delivering business across a range of internal and external sites
- Have the option and ability to work from any site or location where Wi-Fi is enabled

Equipment

- Standard mobile phone
- Laptop computer with standard carry case
- Laptop peripherals - i.e., plug in mouse, keyboard, screen if required
- External network access

2. SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff and others undertaking work on behalf of the CCG who are permitted to use equipment of the organisation at home or other place of work, or third-party computing resources to connect to networked services of the organisation.
Such equipment includes, but is not limited to:

- Laptop computers
- Tablet's or other hand-held devices

- Smartphones

Personal broadband internet/wireless connection

3. POLICY PURPOSE AND AIMS

Requesting Remote Access

Remote access can be requested for any existing staff member or can be requested as part of the setup of a new account.

Requests for remote access should be directed to the IT Service Desk and should originate from the Line Manager of the individual requiring the access. Once logged the IT department will process the request.

Guidelines

Health and Safety
In principle the same considerations should be given to the remote working environment as to the working in the normal office environment. You should ensure your immediate working environment is free of trip hazards, electrical connections are safe etc. It is the employee's duty to always consider the risks surrounding their working environment, and take steps where appropriate. If staff require reasonable adjustments to their remote working you due to a disability, this should be raised with your line manager. Line managers should respond to requests promptly and, where necessary referring to the Occupational Health service. The CCG is committed to supporting the mental health and wellbeing of employees who are working remotely. The HR team can provide employees and managers with links to appropriate resources

Theft

A laptop or other mobile device is a prime target for theft, as they are small, expensive, and generally easy to dispose of.

- You should never leave devices unattended
- You should never leave devices on view in a motor vehicle. Ideally always take equipment with you, however if you have no choice but to leave equipment in a vehicle ensure it is locked in the boot and not visible
- Security of such equipment can also be an issue in a high-risk environment
- An individual carrying what is clearly a laptop bag is a prime target, so wherever possible ensure you are aware of the risks surrounding you. The use of rucksacks or other non-obvious bags to carry a laptop may be advisable in some circumstances

Privacy and Information Governance

The rules applying to information governance in the workplace similarly apply to remote working using IT equipment. You should take all steps that are necessary to ensure that information is not accidentally disclosed.

In particular, ensure that you are not overlooked when using any system. If you are in a public place, then find a location where it is not possible for anyone to see over your shoulder. CCTV is also prevalent in today's world, particularly in the UK, so it is advisable to be aware of any cameras overlooking your point of work that might be able to see information on your screen. It may be possible to purchase a Privacy screen.. These screens fit over the laptop's monitor and reduce the viewing angle of the screen so that it is only visible when looked at squarely to the screen.

The risks associated with a breach of the information governance rules are:

- accidental breach of patient confidentiality
- disclosure of other sensitive/ corporate data to unauthorised individuals
- loss or damage to critical business data
- damage to the organisation's infrastructure and e-services through spread of un-trapped malicious code such as viruses
- the creation of a hacking opportunity through an unauthorised internet access point
- misuse of data through uncontrolled use of removable media such as digital memory sticks and other media
- other operational or reputational damage

Any staff member using alternative communication tools for business purposes must follow the below rules. This applies to any information that is created or received as part of a CCG task, be that communication between teams on work matters, contacting your manager or service delivery.

Before use please ensure:

- you only use alternative communication tools after consulting with your line manager or if in doubt the Information Governance team.
- alternative communication tools are only used where the CCG recommended options are not available and it is critical to service delivery.

While using please ensure:

- Any correspondence created for business purposes is kept separate from any personal conversations that you have. You can do this by creating a new group and adding any relevant officers or partners to it.
- Where possible you should avoid using any alternative to send personal or sensitive data. However, should this be a necessity you will be allowed to do so but you should ensure that you provide only the minimum amount of information needed.

After using please ensure:

- If a conversation contains any decision-making, employee or patient data it should be exported from application and uploaded to the relevant filing system on the Network.
- Once a conversation is no longer required, all parties in the conversation must clear chat / clear messages to remove all versions of it from every device.

Responding to Information Requests

In carrying out CCG business please be aware that any information, even that stored on external applications, is subject to statutory information requests that the CCG may receive such as Freedom of Information requests or Subject Access Requests. This includes:

- any messages between you and your staff,
- any correspondence you created from a personal mobile number for work purpose.

Use of Public Computers or Publicly Available Networks

Great care should be taken using publicly-available equipment, such as an Internet café or hotel PC.

- Ensure that controls exist such that access is controlled. Avoid 'free use' facilities where someone can just walk up and use the device. Most Internet cafés have systems which issue a 'one time' password, which allows access only for a prescribed period of time. If this is the case, also ensure you have allowed sufficient time at the end of your period for 'clearing down' any information you may leave behind.
- If you have any doubts that the device is not properly secured (e.g. does not appear to have any anti-virus software installed), then do not use such equipment
- Facilities will be limited when using public equipment, generally to using Outlook Web Access for reviewing and sending emails
- When you have finished, before closing Internet Explorer make sure you clear the browsing history (depending on the version of Explorer, generally Tools->Internet Options->Clear History), and also remove temporary files (generally Tools->Internet Options->Delete Files). Ensure that the 'Delete All Offline Content' box is ticked.
- If you are using a public available network or 'hotspot', make sure that is a secured network (i.e. requires you to put in a pass key). If it is unsecured, do NOT use it, as any data passing between your PC and the network can be captured.

Storage of Data

- You should never store any data on a non-CCG supplied device. This applies to home PCs or PCs used in hotels or Internet cafes
- Do not store data on diskette, CD or other similar storage device

Memory Sticks

- If data does need to be stored, then use ONLY a CCG-supplied encrypted memory stick .These can be ordered via the IT ordering procedure. subject to a manager's approval.
- 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 member of staff, inform the other individual verbally.
- 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.

Data and Device Encryption

- All mobile devices MUST be equipped with encryption software
- Laptops supplied by the CCG will have this pre-installed
- Other devices, such as Smartphones should also be encrypted. Any device supplied by the IT department will already be encrypted, however devices ordered directly from the manufacturer or distributor may not. If you are in any doubt, please contact the IT Service Desk. As a guide an encrypted device will require a password at power-on, whereas an unencrypted one will not.

Identifying Labels

Remote devices should not carry any identifying labels which immediately indicate they are NHS property. You should also not carry any other identifying paperwork with the laptop, which identifies it as an NHS machine. If possible, always carry paperwork separate from the laptop.

Confidentiality

As the NHSnet is a closed network and access from other networks is very strictly controlled, staff should be aware that the greatest risk to security is posed by those within the network, and not by outsiders. The NHSnet cannot protect systems from the actions, legitimate or otherwise, of other users. Therefore, all staff should be especially aware of the CCG's security and Internet and E-mail policies. Staff should also ensure that they are meeting the requirements of the Data Protection Act 2018 and the General Data Protection Regulation and at all times behave in accordance with UK law.

Staff working on CCG or associated organisations material/work must at all times take extreme care to ensure that confidentiality is maintained and follow appropriate policies.

Sensitive and confidential material must not be taken out of the conventional workplace without prior approval by a member of staff's line manager

Incident Reporting

Any incident which has or you believe may have compromised the integrity of the CCG information systems through remote working should be reported through the existing incident management process. This would include, but is not limited to:-

- Loss or theft of any supplied equipment
- Accidental loss or disclosure of information such as login names, passwords or PIN numbers that could cause the CCG information systems to be compromised.
- Loss or disclosure of any other confidential information.
- Loss or theft of equipment should be reported to the IMT Service Desk immediately. This will ensure that steps can be taken to prevent the equipment being used on the CCG network, and in some cases allow the equipment to be disabled remotely.

4. IMPACT ANALYSIS

4.1 Equality

This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities. As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

- Employees with disabilities may require reasonable adjustment to methods of working or their working environment under the provisions of the Equality Act. Such reasonable adjustments apply equally to a home worker's working environment as for office-based staff

4.2 Bribery Act 2010

NHS Hull Clinical Commissioning Group has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from The Bribery Act 2010.

The Bribery Act 2010 makes it a criminal offence to bribe or be bribed by another person by offering or requesting a financial or other advantage as a reward or incentive to perform a relevant function or activity improperly performed. The penalties for any breaches of the Act are potentially severe. There is no upper limit on the level of fines that can be imposed and an individual convicted of an offence can face a prison sentence of up to 10 years.

For further information see http://www.justice.gov.uk/guidance/docs/bribery-act-2010-quick-start-guide.pdf.

If you require assistance in determining the implications of the Bribery Act please contact the Local Counter Fraud Specialist on telephone number 01482 866800 or email at nikki.cooper1@nhs.net.

Due consideration has been given to the Bribery Act 2010 in the development of this policy and no specific risks were identified.

5. NHS CONSTITUTION

5.1 The CCG is committed to: Designing and implementing services, policies and measures that meet the diverse needs of its population and workforce, ensuring that no individual or group is disadvantaged.

5.2 This Policy supports the NHS Constitution as follows:

The NHS aspires to the highest standards of excellence and professionalism in the provision of high-quality care that is safe, effective and focused on patient experience; in the planning and delivery of the clinical and other services it provides; in the people it employs and the education, training and development they receive; in the leadership and management of its organisations; and through its commitment to innovation and to the promotion and conduct of research to improve the current and future health and care of the population.

6. ROLES / RESPONSIBILITIES / DUTIES

Review and Maintenance -	Senior Information Governance Specialist
Approval:-	Integrated Audit & Governance Committee
Local adoption:-	Line managers (in scope)
Compliance:-	All staff and contractors (in scope)
Monitoring:-	Service Desk, System Engineers, Line Managers

7. IMPLEMENTATION

The policy will be disseminated by being made available on the internet and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

8. TRAINING AND AWARENESS

Staff will be made aware of the policy via the website.

9. MONITORING AND EFFECTIVENESS

The effectiveness of this Policy will be monitored, where there is a suspected issue

an investigation will be performed and staff found to be breach guidance may be subject to disciplinary actions.

10. POLICY REVIEW

This policy will be reviewed within two years of the date of implementation, and in accordance with the following on an as and when required basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

11. REFERENCES

This policy should be used in conjunction with the following policies:

- Acceptable Computer Use Policy
- Data Protection and Confidentiality Policy
- Equality and Diversity Policy

APPENDICES

Annex A – FAQ

What is an Authentication Token?

An authentication token is a small device that is associated with your personal network login account. When you are issued a token you will be required to enter a personal identification number (PIN) upon its first use. When the token is used in conjunction with your network login and password for remote access to the network, you are only given access if the following details are entered correctly:-

- Your Personal Login Name or Username (this is the same login name you use to access the network when at Trust premises)
- Your Personal Password
- Your Token Pin

Annex B – Guidance while working remotely

All staff

- Users must take precautions to ensure that no breach of confidentiality or inappropriate disclosure can arise as a result of unauthorised access by others resident at, or visiting the remote location.
- Under no circumstances must anyone other than the authorised user be allowed access to the connection, even for seemingly harmless activities.
- Users must ensure that PC is located in a discrete location where the screen is not
- easily overlooked.
- Users must take particular care to log off from the remote connection when not in use.
- Users are responsible for the security of personal logins and password security. **You should never tell anyone your personal network password under any circumstances.**
- Users are responsible for your Authentication token and your associated PIN. **You must never tell anyone your PIN. If you suspect someone knows your PIN you must notify the IT Service Desk immediately in order to have the token disabled.**
- Users are responsible for any loss of their Authentication Token. **If you lose your Authentication token you must report this to IT service Desk immediately.**
- You or your department are responsible for any costs associated with lost or stolen Authentication tokens.
- Equipment should not be left in vehicles overnight.

HR / Corporate Policy Equality Impact Analysis:	
Policy / Project / Function:	Mobile Working Policy & Guidelines V2.0
Date of Analysis:	14/04/2020
Completed by: **(Name and Department)**	Hayley Gillingwater Senior Information Governance Specialist
What are the aims and intended effects of this policy, project or function?	The overall purpose of the policy is to set out the CCG's approach to the mobile working within the workplace. The policy will also set out guidance to staff and managers about their responsibilities in relation to mobile working.
Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?	No
Please list any other policies that are related to or referred to as part of this analysis	Acceptable Computer Use Policy Data Protection and Confidentiality Policy General Data Protection Regulation (GDPR) Data Protection Act 2018
Who will the policy, project or function affect?	All staff
What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Consultation on the new policy has taken place nationally and locally. Consultation on the updated policy has taken place locally.
Promoting Inclusivity and Hull CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation?	The policy does not directly promote inclusivity but provides a framework for the CCG's approach to the security and transmission of personal confidential data and Information within the workplace, ensuring staff are supported by management and health professionals

How does the policy promote our equality objectives: 1. Ensure patients and public have improved access to information and minimise communications barriers 2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job 3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve 4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs 5. To demonstrate leadership on equality and inclusion and be an active champion of equalities in partnership programmes or arrangements	

Equality Data	
Is any Equality Data available relating to the use or implementation of this policy, project or function? Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected Characteristics* – referred to hereafter as *'Equality Groups'.* Examples of *Equality Data* include: (this list is not definitive) 1: Recruitment data, e.g. applications compared to the population profile, application success rates 2: Complaints by groups who share / represent protected characteristics	Yes ☐ No x Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). If you answered No, what information will you use to assess impact? **Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.**

4: Grievances or decisions upheld and dismissed by protected characteristic group 5: Insight gained through engagement	

Assessing Impact

Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups?
(Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)

Protected Characteristic:	No Impact:	Positive Impact:	Negative Impact:	Evidence of impact and, if applicable, justification where a *Genuine Determining Reason*[1] exists (see footnote below – seek further advice in this case)
It is anticipated that these guidelines will have a positive impact as they support policy writers to complete meaningful EIAs, by providing this template and a range of potential issues to consider across the protected characteristics below. There may of course be other issues relevant to your policy, not listed below, and some of the issues listed below may not be relevant to your policy.				
Gender	X			This policy applies to all regardless of gender
Age	x			This policy applies to all regardless of age.
Race / ethnicity / nationality	X			This policy applies to all regardless of race/ethnicity/nationality.
Disability	x			This policy applies to all regardless of disability. Employees with disabilities may require reasonable adjustments to methods of working or their working environment under the provisions of the Equality Act. Such reasonable adjustments apply equally to a home worker's working environment as for office-based staff.
Religion or Belief	x			This policy applies to all regardless of religion or belief.
Sexual Orientation	x			This policy applies to all regardless of sexual

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

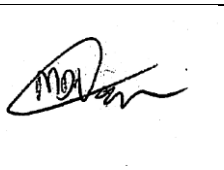
				orientation.
Pregnancy and Maternity	x			This policy applies to all regardless of pregnancy/maternity.
Transgender / Gender reassignment	x			This policy applies to all regardless of transgender/ gender reassignment.
Marriage or civil partnership	x			This policy applies to all regardless of marriage or civil partnership.

Action Planning:

As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?

Identified Risk:	Recommended Actions:	Responsible Lead:	Completion Date:	Review Date:
As the policy is written in English there is a potential impact on employees whose first language is not English and therefore may struggle reading the policy.	The CCGs internal 'portal' and external website signpost individuals to alternative formats such as large print, braille or another language.	CCG Communications	Updating of this facility is ongoing	Next Policy review – April 2022.

Sign-off
All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs
I agree with this assessment / action plan
If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:



Signed:

Date: 03.06.20