NHS
Harrogate and Rural District
Clinical Commissioning Group

# Mobile Working Policy and Guidelines

## November 2017

| | |
|---|---|
| **Authorship:** | **Chris Wallace – Information Governance Manager** |
| **Committee Approved:** | Audit Committee |
| **Approved date:** | November 2017 |
| **Review Date:** | November 2020 |
| **Equality Impact Assessment:** | Completed |
| **Target Audience:** | Council of Members, Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract |
| **Policy Number:** | 039 |
| **Version Number:** | 3.0 |

**The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.**

## 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 Intranet |
|---|---|---|---|---|
| 1.0 | C Wallace | Document created | | |
| 2.0 | IG Officer | Addition of form to record equipment issued | IGSG March 2015 | |
| 2.0 | IG Officer | No Changes Required | IGSG Sept 2015 | |
| 3.0 | IG Officer | To update for the requirements of the General Data Protection Regulation | Audit Committee November 2017 | January 2018 |

**CONTENTS**

## 1 INTRODUCTION

The Harrogate and Rural District Clinical Commissioning Group (thereby known as the CCG) are much smaller organisations with less funds then that of their predecessor PCT organisations. Mobile working allows the CCG to make cost savings while ensure that staff remains interconnected and able to work from almost anywhere.

The CCG has therefore adopted three levels of agile working with all staff falling into one of these 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.
- Use of Fixed Desktop Computer, or 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 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 wifi is enabled

**Equipment**

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

**Flexible Plus**

Flexible Plus workers will:

- Have the ability to effectively deliver their work utilising space across a range of CCG buildings or locations where wifi is available
- Spend most of their time working 'on the move'; accessing information or conducting community/client/patient based activities, working across a range of operational / business sites and coming into offices only for meetings or other specific events
- Have the option and ability to work from any site or location regardless of whether there is wifi.

**Equipment**

- Smart Phone
- Laptop computer with standard carry case
- External network access
- 3G dongle (SIM) - One off initial cost as well as monthly charge

While there are differences between these staffing groups any CCG member of staff can request remote access. Willful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.

## 2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

## 3 IMPACT ANALYSES

### 3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

## 4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG etc who are permitted to use equipment of the organisation at home or other place of

work, or who may use their own personal or third-party computing resources to connect to networked services of the organisation.
Such equipment includes, but is not limited to:

- Laptop computers
- PDA's or other hand-held devices
- Smartphones

## 5 POLICY PURPOSE & 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 IMT Service Desk and should originate from the Line Manager of the individual requiring the access. Once logged the IMT 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.

### 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 leave equipment in a vehicle ensure it is locked in the boot and not visible
- Such equipment can also be an issue in a high-risk environment, such as a housing estate. 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 similar apply to remote working using IT equipment. You should take all steps that are necessary to ensure that information is not 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. Privacy screens are available on request from the Information Governance Team. 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 data of the organisation 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

**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 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 are available by request from the IMT department, 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 IMT 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 IMT 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 make a note of any serial or asset numbers on the devices you have been issued with. These will be required when any loss or theft is reported.

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 1998 and General Data Protection Regulation 2016, 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 Trust 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 within 24 hours of being identified 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.

## 6 ROLES / RESPONSIBILITIES / DUTIES

| | |
|---|---|
| Review and Maintenance: | Information Security Officer |
| Approval: | CCG Management Team |
| Local adoption: | Line managers (in scope) |
| Compliance: | All staff and contractors (in scope) |
| Monitoring: | Service Desk, System Engineers, Audit |

## 7 IMPLEMENTATION

The policy will be disseminated by being made available on the intranet 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 & AWARENESS

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

## 9 MONITORING & AUDIT

Adherence to this policy will be monitored through the incident reporting system and also through standard IMT monitoring KPI's. 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 in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

## 11 REFERENCES

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

Acceptable Computer Use Policy
Data Protection and Confidentiality Policy

## Annex A – FAQ

What is a Authentication Token?

A 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
- The Secure Token rolling Number

## 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 form 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 IMT 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 IMT 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

## Records of Mobile Equipment Issued

| | |
|---|---|
| Name : | |
| Job Title : | |
| Line Manager and Directorate : | |
| Contact Telephone : | |
| | Date Issued : |
| **Please Tick If You Use :** | |
| Laptop (specify make, model and serial no.) | |
| Tablet (specify make, model and serial no.) | |
| USB pens / drives (memory sticks) - Please give reference no. if one available | |
| VPN (RAS) Token (specify serial no.) | |
| iPhone (please specify if this is mobile and data)<br>• Mobile phone (please specify number) | |
| • SIM Number | |
| • IEMI Number | |

This form must be completed by all staff using portable equipment, including personally owned devices when accessing the network remotely using VPN (RAS) Token.

I confirm that I have received a portable device and have read, understood and will comply with the Mobile Working Policy.

| | | |
|---|---|---|
| Print Name : | Signature : | Date : |
| Manager : | | |

**Appendix 1**

| 1. Equality Impact Analysis | |
|---|---|
| **Policy / Project / Function:** | Mobile Working Policy and Guidelines |
| **Date of Analysis:** | 13/01/14 |
| **This Equality Impact Analysis was completed by: (Name and Department)** | C Wallace - IG Manager – CCG IG Team |
| **What are the aims and intended effects of this policy, project or function ?** | This Policy defines the types of worker .e.g. fix desk or flexible and provides guidance to staff who work remotely. |
| **Please list any other policies that are related to or referred to as part of this analysis?** | |
| **Who does the policy, project or function affect ?**<br><br>Please Tick ✔ | Employees ☒<br>Service Users ☐<br>Members of the Public ☐<br>Other (List Below) ☒<br>Any users of CCG IT equipment |

| 2. **Equality Impact Analysis: Screening** | | | | | |
|---|---|---|---|---|---|
| | Could this policy have a positive impact on… | | Could this policy have a negative impact on… | | Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact |
| | Yes | No | Yes | No | |
| **Race** | ☐ | ☒ | ☐ | ☒ | |
| **Age** | ☐ | ☒ | ☐ | ☒ | |
| **Sexual Orientation** | ☐ | ☒ | ☐ | ☒ | |
| **Disabled People** | ☐ | ☒ | ☐ | ☒ | |
| **Gender** | ☐ | ☒ | ☐ | ☒ | |
| **Transgender People** | ☐ | ☒ | ☐ | ☒ | |
| **Pregnancy and Maternity** | ☐ | ☒ | ☐ | ☒ | |
| **Marital Status** | ☐ | ☒ | ☐ | ☒ | |
| **Religion and Belief** | ☐ | ☒ | ☐ | ☒ | |
| **Reasoning** | | | | | |
| **If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7** | | | | | |