NHS
Leeds
Clinical Commissioning Group

Mobile Working Policy and Guidelines

Version:	1.4
Ratified by:	Audit Committee
Date ratified:	20 October 2021
Name & Title of originator/author:	Karen Rowe, Information Governance Manager
Name of responsible committee/individual:	Information Governance/ Business Intelligence/IT Committee
Date issued:	August 2020
Review date:	October 2023
Target audience:	All Staff

Executive Summary

This policy aims to set out an appropriate and safe way to work remotely, out of the office, from home or other designated workplace. The controls detailed ensure that personal and special categories of data are protected when working outside WIRA house. As the CCG becomes a more agile organisation and information can be protected by technological and procedural means, this enables our people to work in all manner of places to ensure a work/life balance but also to strengthen business and service continuity.

Equality Impact Assessment
This policy applies to all employees, Governing Body members and members of NHS Leeds Clinical Commissioning Group irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Table of Contents

1 Introduction

Employees may be required to work at a location other than their official base for the purposes of efficiency, effectiveness and business continuity. This policy sets out the security considerations to apply when working at locations other than the assigned workplace

2 Aims

The aim of this policy is to enable the CCG to protect information assets and detail actions for employees in the management of CCG equipment and information when working away from assigned workplace.

3 Scope

This policy applies to all CCG staff including staff on temporary or honorary contracts, seconded staff, volunteers, pool staff, Governing Body members, students and others undertaking work on behalf of the CCG.

4 Accountability and Responsibilities

4.1 Senior Information Risk Owner (SIRO)

The SIRO has organisational responsibility for all aspects of risks associated with information governance, including those relating to confidentiality and data protection.

4.2 Line Managers

Line managers are responsible for:

- reviewing where business need has identified that staff need to work flexibly either across sites and/or at home.
- determining with staff how such provisions are to be delivered in accordance with this and associated policies.

4.3 All Staff

All staff are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment including whilst working remotely.

All staff must follow and comply with this policy and all associated policies to ensure that remote access and all related considerations regarding work environment and role have been determined.

The accountability and responsibilities are set out in more detail in the Information Governance Policy and Management Framework which must be read in conjunction with this policy.

All staff must complete their Data Security Awareness training on an annual basis.

5 Processes for Ensuring Network Security

5.1 Remote Working or Working from Home

Working remotely must be authorised by line management and comply with Information Governance policies. Remote access requests should be directed to Leedsccg.gpit@nhs.net

5.2 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 working environment, and take steps where appropriate.

5.3 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 allow anyone else to use your laptop at home, or elsewhere.
- 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
- You should never store personally identifiable or corporately identifiable paperwork in your laptop bag.

All equipment must be returned in a similar condition at the point that the employee, agency worker or contractor ceases their role with the CCG

5.4 Privacy and Information Governance

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

In particular, ensure that no unauthorised personnel can overlook you and your equipment when using any system in a public place. 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 or overhear any confidential conversations. Privacy screens should be used where possible; 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 personal or special category data or other OFFICIAL data to unauthorised individuals
- Loss or damage to critical business data,
- Damage to the organisation's infrastructure and services through spread of 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 memory sticks and other media

- Loss or damage to CCG equipment
- Other operational or reputational damage

5.5 Use of Public Computers or Publicly Available Networks

You must not use publically available equipment to access CCG information including email, such as a café computer, or hotel PC.
If you are using a public, secured network from your own device, ensure it requires you to register. If it is unsecured, do NOT use it, as any data passing between your PC and the network can be captured.

5.6 Storage of Data

- You should never store any data on a non-CCG supplied device.
- Do not store data on unencrypted CD, USB or removable media device.
- If data is stored on an encrypted device, ensure that it is deleted as soon as it is no longer required.

5.7 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.

5.8 Confidentiality

Staff should be aware that the greatest risk to security is posed by those within the network, and not by outsiders. Therefore, all staff should be especially aware of the CCG's Information Security, and Email policies. Staff should also ensure that they are meeting the requirements of the UKGDPR and the Data Protection Act 2018, 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 CCG 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

5.9 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 as soon as possible and always 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 Informatics IT department 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.
- Loss or compromise of any confidential information documented on paper

5.10 Broken and old equipment

Broken and old equipment, including mobile phones, should always be returned to the CCG to be disposed of securely

6 Implications and Associated Risks

All associated risks resulting from the implementation of the Policy should be assessed and where necessary recorded on the appropriate risk register.

7 Education and Training Requirements

Data Security and Awareness training must be completed on an annual basis for all staff and must be completed for new employees within one week of commencement of employment.

8 Monitoring Compliance and Effectiveness

Compliance with this policy will be monitored through the incident reporting system and through standard IT investigations. Staff found to be in breach may be subject to disciplinary actions.

Reporting of breaches of the policy will be recorded and discussed in Information Governance / Business Intelligence and IT Committee meetings. Additional training will be provided for anyone found to be in accidental breach.

The Audit Committee is responsible for monitoring compliance against this policy.

9 Associated Documentation

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

- Confidentiality and Data Protection Policy
- Information Security Policy
- Network Security Policy
- Email policy
- Internet and Social Media policy
- Confidentiality: Code of Conduct
- Acceptable Use policy

Appendices

A Policy Consultation Process:

Title of document	Mobile Working Policy and Guidelines
Author	Karen Rowe
New / Revised document	Revised
List of persons involved in the consultation process:	Abi Dakin Karen Rowe Steve Creighton Louise Whitworth Cheryl Mitchell

Addendum to Mobile Working Policy

Introduction

In certain circumstances it will be necessary for staff to work from home, possibly for long periods of time. This addendum sets out the security levels required to maintain the confidentiality and security of data outside of the office environment.
There are more risks to information and equipment associated with remote working than being in the office. Even in special circumstances you must follow UK Data Protection Legislation whilst working remotely.

Your Responsibilities

You are responsible for the security of your equipment and information when you are working from home, you need to adhere to the below:

- When taking information or equipment home with you, or returning it, make sure it is kept out of sight at all times, for example in a bag that can be secured by a zip or button fastening. If traveling in a car bags should be stored out of sight. If traveling on public transport ensure you keep any equipment and/or records on your person at all times.

- Only use approved equipment – the laptops issued by the CCG

- Work equipment should be set up in an area where you have some privacy to handle calls and emails that may involve the processing and/or handling of a patient's health information.

- Make sure that any patient information is not viewed or overheard by anyone else in your home. You can do this by ensuring that other members of the household are not able to access your work equipment when in use. Always lock your screen when you are away from your laptop.

- If making notes please use your laptop to do this where possible rather than a paper notepad.

- Place all work documents and/ or paper records out of sight when not in use, where possible in a secure lockable bag or storage unit. If you have any paper documents or notes these should be stored separately to your laptop.

- Where you have created any new information in paper ensure when possible it is transferred to the appropriate electronic system and any paper copies are disposed of in confidential waste bins in the office at the earliest opportunity. Do not dispose of any personal data at home.

.

Communication tools

Where it is not possible to meet with colleagues or patients, alternative methods of communication are required. Wherever possible Microsoft Teams should be used, however it is recognised that this may not be accessible to all. It has therefore been agreed that other methods such as WhatsApp may be used.

Your Responsibilities
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 people to it.
- Where possible you should avoid using any alternative method 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.