NHS
Leeds
Clinical Commissioning Group

Mobile Working Policy and Guidelines

Version:	1.2
Ratified by:	Information Governance Committee
Date ratified:	13/3/2019
Name & Title of originator/author:	Abi Dakin, Cyber Assurance and Compliance Manager
Name of responsible committee/individual:	Audit Committee
Date issued:	19/03/2019
Review date:	March 2021
Target audience:	All Staff

Executive Summary

The Mobile Working Policy and Guidelines document 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 further bolster business and service continuity.

Table of Contents

1 Introduction

Employees occasionally do not work at their assigned workplace and require IT equipment in order to work effectively. 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 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 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
- Tablets or other hand-held devices
- Smartphones

4 Accountability and Responsibilities

4.1 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) has organisational responsibility for all aspects of risks associated with information governance, including those relating to confidentiality and data protection. These duties include:

- Take ownership of the organisations Information Security Policy and risk assessment process
- Act as advocate for information risk on the Board and provide written advice to the accountable officer (if this is not the SIRO) on the content of the Annual Governance Statement in regard to information risk
- Understand how the strategic business goals of the organisation may be impacted by information risks
- Oversee the development of an Information Security Policy, and a strategy for implementing the policy within the existing Information Governance Framework.
- Take ownership of risk assessment processes for information risk, including the review of the annual information risk assessment to support and inform the Annual Governance Statement
- Ensure that identified information security threats are followed up and incidents managed
- Review and agree action in respect of identified information risks of resources, commitment and execution and that this is communicated to all staff
- Provide a focal point for the resolution and/or discussion of information risk issues
- Ensure the Board is adequately briefed on information risk issues

- Be required to undertake and pass strategic information risk management training at least annually
- Ensuring that sufficient resources are provided to support Information Governance
- Defining the organisations policy in respect of Information Governance and records management, taking into account legal and NHS requirements

4.2 Line Managers

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

4.3 All Staff

- 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 Strategy and Policy and Management Framework which must be read in conjunction with this policy.

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
- Information taken off site where held on portable devices must be secured and backed up regularly to the appropriate CCG server
- Remote access once authorised by line management should be directed to the IT Service desk IT_servicedesk@embedhealth.co.uk 0345 1408000

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 machine 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 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 is advisable to be aware of any cameras overlooking your point of work that might be able to see information on your 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, 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
- 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**

As the N3 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 N3 network 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 email policies. Staff should also ensure that they are meeting the requirements of GDPR and the Data Protection Act, 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 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.

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

Information Governance training including Cyber is mandatory and must be completed on an annual basis for all staff.

8 Monitoring Compliance and Effectiveness

Adherence to this policy will be monitored through the incident reporting system and also through standard IT investigations 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 Committee meetings. Additional training will be provided for anyone found to be in accidental breach.

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

Appendices

A 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.

B Policy Consultation Process:

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