Mobile Working Policy

February 2021

Authorship:	Senior Information Governance Specialist
Committee Approved:	NHS North Yorkshire CCG Audit Committee
Approved date:	February 2021
Review Date:	February 2024
Equality Impact Assessment:	Yes
Sustainability Impact Assessment:	Yes
Target Audience:	Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	NY-114
Version Number:	1.1

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
0.1	Senior Information Governance Specialist	First Draft	Information Governance Steering Group (IGSG) - January 2021	
0.2	Senior Information Governance Specialist	Second Draft	Audit Committee – February 2021	
1.0	Senior Information Governance Specialist	Final Approved Version		Feb 21
1.1	Senior Information Governance Specialist	Requirement for new starters to complete Data Security training within first week of starting employment	IGSG (May 2021)	May 2021

Contents

1.0 Introduction

NHS North Yorkshire Clinical Commissioning Group (thereby known as the CCG) requires staff to mobile work for the purposes of efficiency, effectiveness and for business continuity purposes. This policy set out the requirements of staff when working away from their main office.

2.0 Purpose

This policy sets out the guidelines for staff that are required to carry out mobile working.

In principle the same considerations should be given to the remote working environment as to the normal office environment. Staff should ensure their 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 to eliminate them where appropriate.

3.0 Definitions / Explanation of Terms

3.1 Mobile Working

Mobile working is when staff work away from their official office base, this can include but is not limited to working at other CCG sites, other NHS organisations, from home and other places as required.

4.0 Scope of the Policy

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 and IPads
- PDA's or other hand-held devices
- Smartphones

5.0 Duties, Accountabilities and Responsibilities

5.1 Accountable Officer

Overall accountability for procedural documents across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective Information Governance Framework, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

5.2 Senior Information Risk Officer Owner (SIRO)

The CCG’s SIRO is responsible for overseeing the implementation of appropriate processes and procedures to ensure that individual’s information can be processed and held securely.

5.3 Caldicott Guardian

The CCG’s Caldicott Guardian is responsible for overseeing and advising on issues of service user confidentiality for the CCG including breaches of confidentiality personal information.

5.4 Corporate Services Manager

Responsibility for the management, development and implementation of policy procedural documents lies with the CCG in partnership with the NECS Information Governance Team

5.5 Line Manager

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to mobile working. They are also responsible for monitoring compliance with this guideline e.g. undertake ad hoc audits to check for inappropriate disclosures, records left out, abuse of passwords etc.

5.6 All Staff

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

Individual staff members are personally responsible for any decision to pass on information that they may make.

All staff are responsible for adhering to the Caldicott principles, Data Protection Legislation, and the Confidentiality Code of Conduct.

Staff will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods (e.g. team brief/team meetings);

All staff are mandated to undertake Information Governance training on an annual basis. This training should be provided as soon as possible and then updated as appropriate in accordance with the Statutory and Mandatory Training Standard and Information Governance Training Needs Analysis.

The CCG must ensure that all contractors and supporting organisations are working to documented contracts or service level agreements that detail their responsibilities in respect of information governance and security, and confidentiality and data protection.

This includes the completion of the Data Security and Protection Toolkit to a satisfactory level.

5.7 Responsibilities for Approval

Audit Committee is responsible for the review and approval of this policy.

6.0 Policy Procedural Requirements

6.1 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 via the ICT service desk and should originate from the line manager of the individual requiring the access. Once logged the ICT department will process the request.

6.2 Privacy and Information Governance

The rules applying to information governance in the workplace similarly apply to remote and mobile working, and 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 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
- Loss of or damage to CCG equipment
- other operational or reputational damage

6.3 Storage of Data

- Data should never be stored on a non-CCG supplied device. This applies to home PCs or PCs used in hotels or Internet cafes
- Never store data on diskette, CD or other similar storage device

6.4 Memory Sticks

- If data does need to be stored, then this should only be on a CCG issued encrypted laptop or a CCG-supplied encrypted memory stick. These are available by request from the ICT department, subject to a manager's approval. All data must then be transferred to the CCG network as soon as is practicable.
- All encrypted equipment has a unique serial number and password assigned. Information held on this equipment 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.

6.5 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 ICT 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 ICT Help Desk. As a guide an encrypted device will require a password at power-on, whereas an unencrypted one will not.

6.6 Identifying Labels

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 always carry paperwork separate from the laptop to prevent cross identification of information.

6.7 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 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 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

6.8 Paper Records

It is essential that staff have appropriate management approval, i.e. the named information asset owner, to remove paper files and other documented information from the CCG and that a record of any records removed is recorded and maintained at the CCG premises.

Staff should ensure that all CCG records removed from the office are kept to an absolute minimum and are transported securely in lockable cases and held securely whilst away from the office. It is essential that such records are not viewed by unauthorised personnel, this includes members of or visitors to the household whilst in working from home. Records must be used confidentially and held securely when not in use to maintain appropriate confidentiality.

6.9 Incident Reporting

Any incident which has or you believe may have compromised the integrity of the CCG information systems or confidential information 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 ICT 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.
- Loss or compromise of any confidential information documented on paper.

6.10 Broken and old equipment

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

7.0 Public Sector Equality Duty

In developing this policy an Equality Impact Analysis (EIA) has been undertaken. As a result of the analysis, this policy,-does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

NHS North Yorkshire CCG aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

8.0 Consultation

This Policy has been reviewed by Information Governance Steering Group prior to approval by the Audit Committee.

9.0 Training

Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test, this must be completed by new employees within one week of commencement of employment. Further specific training may be required in line with job roles delegated to staff.

10.0 Monitoring Compliance with the Document

The CCG will monitor compliance with the policy throughout the year via:

- Monitoring and investigating incidents resulting in a breach of confidentiality. Guidance will be sort from the IG Team as appropriate
- Lessons learnt from incidents will be reflected in policies and procedures as required and communicated to staff via the CCG newsletter.

Audit Committee is responsible for monitoring compliance against policy. This is done via updates provided from the Information Governance Steering Group.

11.0 Arrangements for Review

This policy will be reviewed every three years 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.

12.0 Dissemination

This policy will be published on the CCG's internet and will therefore be available to both staff and the public.

Staff will be made aware of the existence of this policy and all subsequent updates via the staff newsletter.

13.0 Associated Documentation

- Information Security Policy.
- Email and Internet Policy.
- Acceptable Use Policy.
- Data Protection and Confidentiality Policy
- Confidentiality: Code of Conduct

14.0 References

This policy was developed in line with the following practices and legislation:

- Data Protection Act 2018;
- Human Rights Act 1998;
- General Data Protection Regulation 2016
- Health and Social Care Act 2012 and HSC (Safety and Quality) Act 2015.
- The Computer Misuse Act 1990;
- The common law duty of confidentiality;
- National Data Guardian Standards;
- Caldicott principles;
- Information Commissioners Data Sharing Code of Practice

15.0 Appendices

Appendix A – Guidance for remote Working

Appendix A

Guidance for Remote Working

- 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.
- Equipment, files and documents must be held and transported in secure bags/cases whilst away from the office.
- Ensure that all manually information taken out of the office is recorded in the appropriate tracking system.
- 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. If you suspect someone knows your PIN you must ICT Service Desk**
- Users are responsible for reporting the loss of any equipment immediately.
- All breaches to confidentiality must be reported immediately.
- Equipment, files or documents should not be left on show or left in vehicles overnight and must never be left unattended in public places.