NHS
Barnsley Clinical Commissioning Group
Putting Barnsley People First

BARNSLEY CLINICAL COMMISSIONING GROUP'S REMOTE WORKING AND PORTABLE DEVICES POLICY

Version:	2.0
Approved By:	Governing Body
Date Approved:	Feb 2014 (initial approval), March 2016 (review)
Name of originator / author:	Richard Walker
Name of responsible committee/ individual:	Governing Body (Approval) Information Governance Group / QPSC (review)
Name of executive lead:	Vicky Peverelle
Date issued:	
Review Date:	2 years from approval
Target Audience:	Barnsley CCG staff

THIS POLICY HAS BEEN SUBJECT TO A FULL EQUALITY IMPACT ASSESSMENT

Amendment Log

Version No	Type of Change	Date	Description of change
DRAFT		February 2014	
V1		13 February 2014	*Approved by Governing Body*
V2.0	Review	February 2016	*Enhanced clarity of content* *Removal of references to obsolete devices* *Non-acceptable period of time for laptops left in cars changed (shopping trips > extended)*

Remote Working and Portable Devices Policy

Table of Contents

Remote Working and Portable Devices Policy

1. Introduction

- Current models of Health and Social Care administration and delivery, and flexible working practices, are such that staff may need to access Barnsley Clinical Commissioning Group (CCG) information from a location that is not their normal work base. For example, individuals may not have a static work base or they may need occasionally to work away from their normal place of work. In addition, flexible working practices mean that some staff may be working from home on a regular or ad hoc basis.[1]

- Developments in technology are such that it is now possible to process information using various types of portable (mobile) electronic devices such as laptops, tablet computers, smartphones and USB memory sticks enabling staff to work not only at different locations but also while they are 'on the move'. While these developments in technology and changes to working practice bring many benefits they also introduce risks to the organisation, individual staff members and the security of CCG information. Information is no longer retained in the work base where it is automatically backed up, but is potentially accessed or stored from across the region, on a variety of devices. The convenience of these devices, their small size and capacity to hold large amounts of information, presents their greatest risk. They can easily be lost, mislaid or stolen. It is important that information, whether held on mobile devices or accessed remotely, is protected by adequate security.

2. Objective

- The purpose of this policy is to protect CCG information that is processed remotely or is stored on portable devices and to protect staff from inadvertently breaching information security. It forms part of an overall suite of information governance policies and should be read in conjunction with the Information Security Policy in particular.

3. Scope

This policy covers:

- Remote working, that is, working on CCG information or accessing the CCG network in a place that is not your normal work base or work station.
- The use of portable processing devices, which includes portable computers such as laptops and tablet notebooks (for example, ipads), smart phones such as blackberries and iphones, personal digital assistants (PDAs), digital cameras, dictation devices, mobile phones and any other mobile devices which process information.

[1] Working from home should be in accordance with the CCG's policy on Home Working

In particular, the policy covers:

- Connection to the CCG network – remotely and with portable devices
- The processing of CCG information away from CCG premises
- The processing of CCG information on CCG provided portable devices
- The processing of CCG information on personal portable devices
- The secure transfer of information
- The security of portable devices and information
- The use of home computers and personal mobile devices
- The use of portable media and internet access by external visitors (section 14)

4. Compliance With This Policy

- This policy applies to all users of CCG systems and equipment including CCG employees and non-CCG employees who work within NHS Barnsley Clinical Commissioning Group or under contract to it. This includes, but is not limited to, staff on secondment to the CCG, students on placement and people working in a voluntary capacity.
- For convenience, the term 'staff' is used in this document to refer to all those to whom the policy applies.
- All staff are required to comply with this policy.
- This policy is based on current law, NHS Information Governance standards and accepted standards of good practice; your duty to **handle CCG and person identifiable information appropriately** arises out of common law, legal obligations, staff employment contracts and professional obligations.[2]
- The policy should be cross-referenced with other information governance and procedural documents. An up to date list of documents is available on the information governance intranet page. Staff should ensure that they are familiar with the content of this policy.
- Any breaches of this policy may result in your employment or your association with the CCG being terminated. It may also bring into question your professional registration[3] and may result in disciplinary, civil or criminal proceedings.
- If there is anything that isn't clear or which you do not understand in this policy you must contact your line manager, in the first instance, or the Information Governance Lead for further information**.**
- Please note that the procedures and policies outlined in this policy and any related policy may be changed at any time. You will be alerted to this via established CCG communication routes such as team meetings, newsletters, intranet and internet.

5. Generic Responsibilities of Staff and the CCG

- All managers are responsible for ensuring that the staff they manage are aware of the Remote Working and Portable Devices policy and their individual responsibility for complying with it. They should ensure their staff

[2] For example, with the General Medical Council, Nursing and Midwifery Council or Health Professions Council

[3] See note 3 above

are equipped to fulfil those responsibilities; this will include covering it at local induction and by identifying and meeting specific and generic training needs through personal development plans.

- Managers should ensure ALL new staff have signed the Confidentiality and Information Security declaration.[4] Managers are required to countersign this declaration to indicate that they have checked that the member of staff has read the relevant information governance policies and has had an opportunity to ask questions about anything they do not understand.
- Senior managers should ensure that managers within their Service are aware of their responsibilities in relation to informing staff about acceptable standards of information governance.
- All staff must ensure that they are aware of the requirements and standards of behaviour that apply.
- All staff are responsible for reporting information incidents and near misses, including breaches of this policy, using the CCG's incident reporting procedures.
- The CCG's incident reporting process can be obtained from line managers in the first instance. Further information can be obtained from the CCG's Quality Manager or Information Governance Lead.
- The CCG's Information Governance Group is responsible for overseeing the implementation of this policy including monitoring compliance. It is responsible for ensuring it is reviewed periodically.

6. Direct Connection to the CCG Network

- All electronic processing devices connecting directly to the CCG's internal network must be protected by up to date anti-virus software. Where the device does not update automatically, it is the responsibility of the user to ensure that the anti-virus software is up to date.
- Personally owned devices must not be connected directly to the NHS Barnsley Clinical Commissioning Group network.
    - Directly connected means either by wire (network cable) or Wi-Fi.
    - The CCG network means S: or H: drives or intranet
    - Personally owned means devices that are not provided by the CCG
    - Devices includes home personal computers, laptops, notebooks (for example, iPads), media players (such as iPods) and smartphones.

Please note: The CCG has the facility to allow non-CCG provided devices to connect to the internet via a limited access Wi-Fi connection. This should be authorised by the IT Department - Ask the IT Service Desk for advice.

[4] The declaration should be signed by ALL staff who have access to CCG information, that is, ALL staff who work at the CCG and not only those who have access to the CCG network.

7. Remote Connection to the CCG's Network

- Connection to the CCG network remotely (that is, via web services or remote services) requires authorisation by the IT Department and will be subject to authentication procedures specified by them.

8. The Use of Portable Devices

- CCG procurement of portable media must be authorised by the IT Department.
- The use of portable media for work purposes must be in line with CCG policy and authorised by your line manager (and Information Governance/IT Services where appropriate).
- Only portable devices that have been provided/authorised for use by the IT Services Department may be used for work purposes. This includes, but is not limited to, laptops, tablets (for example, iPads), USB sticks, digital dictation machines. Personal smart phones may be used to access NHS mail if protected by appropriate security.
- All portable devices must be protected by appropriate security. Portable devices such as laptops, tablets (for example, iPads), dictation machines smart phones and USB sticks must be encrypted and, where appropriate, have up to date anti-virus software.
- Portable devices used to access NHS mail must be encrypted and have the capacity, and be configured, to allow remote wiping.
- The use of personal USB Memory Sticks is not permitted on CCG equipment or for holding CCG information.[5]
- Portable storage devices (including CDs, DVDs, memory cards and flash drives) containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on CCG equipment.
- Encrypted portable devices may be used to transport information or to enable information to be worked on remotely.[6]
- All information, whether confidential or otherwise, must only be transferred using encrypted portable media.
- Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available.
- Portable devices should not be used as storage devices. This media is a means for transferring data and is not intended to be used for long-term storage nor is it an adequate back up device. The CCG's network provides all users with the facilities to save information securely in folders that are backed-up on a daily basis. Only specific archival CDs/DVDs may be used as long term storage and then only with approval of the Head of Assurance.
- Always transfer information back to its normal storage area as soon as possible. Failure to do this may result in problems with the version control or the loss of information if the portable device is lost or corrupted.

[5] The exception is for external people for the purposes of giving presentations transferring data, for example (see section 15). Unencrypted USB sticks will be read only. Staff who are currently holding CCG data on personal USB sticks should contact the IT Service Desk to enable the information to be transferred to the CCG Network.
[6] Staff who work off-site on a regular basis should request remote access to the CCG Network which will remove the need to use USB sticks for remote working.

- Always remove information from portable media after it is no longer needed.
- In the event of loss, theft or damage to your portable device you should contact the IT Service Desk as soon as possible.
- You must ensure that any suspected or actual breaches of security are reported to the Information Governance Manager directly or via the IT Service Desk. In addition, the incident reporting procedures should be followed.

9. Passwords or passphrases

- Passwords or passphrases must not be written down and kept with the portable device or in an obvious place in an identifiable manner, for example, in your diary under 'laptop password'.
- Always set a password hint to help you to remember. Make sure this is not too obvious.
- If you suspect someone may know your password you should change it immediately. If the device is a pool device, you should inform the pool manager.
- The IT Service Desk can reset passwords during office hours only.

10. Information held on CCG portable devices

- Confidential CCG information may only be held on CCG portable devices with the permission of your line manager and the CCG Information Governance Lead.
- Information must not be stored permanently on portable devices. If it is necessary to use a portable device to process information, the information should be transferred to the CCG server at the earliest opportunity and then deleted from the device.
- Unauthorised software must not be installed onto CCG portable devices.
- Information must be virus checked before transferring onto CCG computers. This will be done automatically for information that is sent via email. (Confidential information sent via email must be encrypted and adhere to the CCGs email policy and its Confidentiality Code of Conduct[7]

11. CCG information held on personal portable devices

- CCG information must not be held on non-CCG equipment, for example, home personal computers, laptops, tablet computers (e.g. iPads), and smartphones unless it is protected by appropriate security and part of a formal explicitly agreed process authorised by the CCG's Information Governance Lead.

[7] Processes such as information transfers of personal confidential data for the purposes of safeguarding should be logged by the Information Governance Lead once, and an information map completed. The IG lead should be consulted for advice on ad hoc transfers of personal confidential data.

12. Security of information and portable devices

Confidential information, whether manual or electronic, and portable devices must be protected by adequate security, for example, they must be:

- Kept out of sight, for example, in the locked boot of the car, when transported.
- Not left unattended, for example, not left in the car boot overnight or for extended periods of time.
- Locked away when not being used.
- Kept secure and guarded from theft, unauthorised access and adverse environmental events particularly when taken home.
- Put back in their normal storage area as soon as possible to minimise the risk of loss (and to enable access by other users).

13. Maintenance of CCG portable devices

- CCG equipment must be returned to the IT Department for a “health check” at regular intervals as specified by the IT Department or at their specific request.

14. External visitors to the CCG

- External visitors, for example, lecturers, contractors, company representatives, patients or their representatives etc. must not connect any device, including USB sticks and laptops, or insert any media to any equipment belonging to the CCG without authorisation.
- The staff member responsible for the visitor may give this authorisation but they must ensure that the device is virus-scanned before any documents are opened. If a virus alert is generated, the member of staff is to stop using the device and inform the IT Service Desk immediately.
- Unencrypted USB sticks will be accessible as read only.
- Wi-Fi access to the internet is available via a guest Wi-Fi account (ask the IT Service Desk/ Reception for details)

15. Further information

- Further information can be obtained from the CCG’s Information Governance Lead.
- Questions about the use of portable devices or any problems in accessing the CCG system should be directed to the IT Service Desk. Support is available during opening hours. There is no out of hours or home support.

Equality Impact Assessment 2013

Title of policy or service	Remote Working and Portable Devices Policy	
Name and role of officers completing the assessment	*Julie Eckford, IG Specialist (initial assessment) and Gershon Nubour (as part of review Feb 20016) – as changes to the policy were minimal no change to the EIA is proposed.*	
Date assessment started/completed	21.01.14	21.01.14

1. Outline	
Give a brief summary of your policy or service • Aims • Objectives • Links to other policies, including partners, national or regional	The policy aims to raise CCG staff awareness of the CCG's expectations in relation to the appropriate handling of information when working remotely and in the use of portable devices to: • Ensure information is handled appropriately and in a secure and confidential manner • Reduce the risk of adverse incidents • Prevent staff inadvertently causing an IG incident through non-compliance of CCG policy The policy links to law such as data protection law, guidance issued by organisations such as DH, Information Commissioner's Officer and Cabinet Office, ISO security standards and other CCG IG policies including information security, email and confidentiality code of conduct.

2. Gathering of Information

This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.

	What key impact have you identified?			What action do you need to take to address these issues?	What difference will this make?
	Positive Impact	**Neutral impact**	**Negative impact**		
Human rights		Y			
Age		Y			
Carers		Y			
Disability		Y			
Sex		Y			
Race		Y			
Religion or belief		Y			
Sexual orientation		Y			

Gender reassignment		Y			
Pregnancy and maternity		Y			
Marriage and civil partnership (only eliminating discrimination)		Y			
Other relevant group		Y			

Having detailed the actions you need to take please transfer them to onto the action plan below.

3. Action plan				
Issues identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication			
When will the proposal be reviewed and by whom?	The EIA will be reviewed when the policy is reviewed. The Head of Assurance is responsible for ensuring the review takes place. This policy will be reviewed not later than 2016.		
Lead Officer	Richard Walker	**Review date:**	March 2016