NHS

Bolton Clinical Commissioning Group

Agile Working Policy

Policy Number	AGILEWOR001
Target Audience	CCG Staff
Approving Committee	IM&T Operations Board CCG Executive
Date Approved	April 2015
Last Review Date	October 2016
Next Review Date	April 2018
Policy Author	GMSS IG Team
Version Number	Final V1.1

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
V1.0	30/4/14	CCG Executive	Approved
V1.1	25/10/16	IMT Ops Board	Review
V1.1	Nov 16	Staff Forum	Review

Analysis of Impact Effect completed:	By:	Date:

Contents

1 Introduction

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation, service continuity and overall success of the CCG.

The CCG acknowledges that we must demonstrate to third parties our knowledge and expertise in security technology and implementing it. To achieve this it is vital and recognised that we must protect our own assets as well as the environment.

The CCG is committed to providing a range of flexible working options for employees in order to maintain a committed and skilled workforce, able to deliver high quality, cost effective services in an environment which maximises opportunities for employees to balance work and personal commitments.

This policy outlines the methods used for agile working.

1.1 Objective

To ensure that the CCG and its staff comply with legislation and NHS standards in respect of information security and in particular the requirements of the NHS in respect of securing personal data and CCG equipment which has to be transferred between departments, sites or other organisations and which is to be used in locations other than in CCG premises.

It is intended that the CCG complies with NHS and legal requirements for the securing of all information and physical assets whilst in transit and in use in locations outside the CCG's Premises. By doing so the CCG seeks to ensure the:

- Confidentiality of personal information
- Integrity of information
- Availability of information
- Security of Physical Assets.

1.2 Scope

The following information is applicable to all staff that use mobile devices such as Laptops, Memory Sticks, tablets, smart phones, cameras, mobile phones, satellite navigation systems and any other piece of electronic equipment capable of holding names, addresses or other corporate information.

This policy covers all types of agile working, whether fixed or 'roving' including:

- Travelling users (e.g. Staff working across sites or are temporarily based at other locations).
- Home workers (e.g. CCG Managers, or Clinicians).
- Non NHS staff (e.g. Social Services, contractors and other 3rd party organisations).

In addition it is recognised that not all information used outside the CCG's premises is accessible through computer or electronic means. Some of that information can be paper based, i.e. health records for seeing patients at other locations or in the patient’s own home, or staff files being used by managers whilst working at home.

2 Other Relevant Procedural Documents

This policy should be read in conjunction with the following documents:

- Acceptable Use Policy
- Information Governance Policy
- Freedom of Information Policy
- Confidentiality and Data Protection Policy
- Corporate Information Security Policy
- Disciplinary Policy and Procedure

3 Roles and Responsibilities

The Chief Officer has ultimate responsibility for the implementation of the provisions of this policy. As the ‘Accountable Officer’ they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements.

Overall responsibility for the security of information lies with the Senior Information Risk Owner (SIRO) who will delegate the responsibility for managing the development and implementation of procedural documents to the IT Service Supplier and line managers within the CCG.

Line managers will take responsibility for ensuring that the Agile working Policy is implemented within their team or directorate.

It is the responsibility of each employee to adhere to the policy. Implications for deliberate loss/damage to any equipment or failure to comply with this policy will result in disciplinary action that may lead to a financial penalty.

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, for example, team meetings;
- Induction Process.

All staff are mandated to undertake the “Introduction to Information Governance” e-learning module. Information Governance training is required to be undertaken on an annual basis.

Failure to complete the required IG training may result in equipment being withdrawn until the training has been completed.

4 Security of Corporate Information

In order to ensure adherence to the Data Protection Act (1998) the following guidelines must be followed:

- As a general principle of good practice patient or staff identifiable information should not be stored on a mobile computer and certainly must not be stored on one unless it is encrypted to the standards required in the Acceptable Use Policy.
- Under no circumstances should any patient based personal information be stored on any mobile device other than equipment provided by the CCG
- Mobile phones containing cameras, personal or work provided will not be used to take or store patient images or to transmit such images. Similarly no patient information will be stored on personally owned equipment mobile devices.

If PCD has to be stored on a mobile computer then the general principles about sensitive information given above must be followed.

- PCD obtained through work must only be stored on computers, electronic equipment or electronic media that are the property of the CCG and therefore are subject to the policies and procedures of the CCG.
- Loss of a mobile computer holding confidential information must be reported following the CCG Incident Reporting procedure as soon as possible. The CCG has responsibility for informing staff or patients if their personal information has been disclosed unlawfully.
- Devices holding sensitive information must be encrypted in order to safeguard the information against unauthorised access. Encryption must be done to the standards currently required by the CCG, as detailed in the Acceptable Use Policy.
- Sensitive information should be removed from the mobile device as soon as practically possible.

Patient identifiable information on mobile devices should be kept to a minimum i.e. use a CCG reference/NHS number instead of a name wherever possible, this is to reduce the risk of breach of confidentiality if the mobile device is lost or stolen.

Information should generally not be stored on mobile devices as such devices are not normally backed up.

All mobile devices must be authorised for use by both the CCG and Greater Manchester Shared Services (GMSS) IT Service Desk before connection to either a PC or the network is allowed.

Mobile devices should be password protected to ensure that unauthorised use cannot occur. Passwords should not be shared. If your password is compromised please report immediately to the IT Service Desk.

Virus protection software must be installed, active and up to date.

4.1 Manually Held Records

As part of agile or mobile working, it is often necessary that paper based records are available. This would be the case for treating patients in their own home, in the case of clinical records, or when attending tribunals, in the case of staff records.

- It is necessary that these records are handled with due care and responsibility and the following points may assist in this:
- Use a case or sealed envelope or wallet to ensure the papers are kept together and nothing can blow away.
- Don’t leave files in an unattended car, even when they are locked in the boot and out of sight.
- Transport documents directly to and from the place of work to the client’s address. Don’t make stops, for example at the local supermarket.
- Return files to the work location at the end of the day or as soon as is practicable.
- Don’t take them home unless absolutely necessary.

However, locally this may need to be carefully considered if it would cut down the number of visits someone can make because of extra travelling to collect the documents at the start of the day. Local policies or procedures will identify those occasions on which the department management will allow such exceptions to the base rule of not taking PCD home. These procedures should be authorised at director level.

If documents are taken home at the end of the day, they must not remain in the car, even if it is locked in the garage. Bring the documents into the house and store them in what you consider to be a safe location. This should be somewhere where other occupants of the house will not casually look through them. A possible location would be where you keep your purse or wallet whilst in the house. They should not be left adjacent to doors or windows.

If visiting a number of clients in the course of the day, consider taking all files with you to each visit, rather than leaving in car.

Travel with car doors locked. A boot could easily be opened by someone at a set of traffic lights, as could a passenger door.

4.2 General Principles for Agile Access

As a general principle, PCD or sensitive information will not be taken off site and used for agile working. This includes manual records and equipment needed to access such electronically held records.

However there are going to be exceptions to this where it is necessary for the purposes of enabling relevant work to be undertaken i.e. care home visits. For these, papers or the computers necessary to access such information, will have to be carried around.

Under those circumstances a member of staff must not make an arbitrary decision to remove those documents, but for regular occasions local policies and procedures must be developed for the handling of the notes and information.

There will be occasions when it is necessary for staff to take notes or sensitive information home, in order to make an early morning appointment at patient’s homes, or in the evening when late appointments prevent documents being safely returned to their normal library location. Again, if locally allowed, the local procedures must document what is permitted. However it is re-iterated that as a default this is not an acceptable practice.

On an occasion which constitutes an unusual event i.e. when a member of staff is required to undertake work on a one off basis outside of the CCG, and which necessitates the use of sensitive or personal data, the authority to take the information or the equipment necessary to access that information must be documented. This authority will be granted by their line manager and will include the date and time during which that information is removed from site, the nature of the information to be removed and the reasons why it is being allowed to be removed. Similar information will also be recorded for the removal of equipment necessary to access such information for agile working.

In all instances where sensitive information has to be taken, or accessed off site, the user must have completed the mandatory Information Governance training and show an understanding of the security issues at stake.

Any local policy approving the use or removing of sensitive information from the CCG's premises must be approved by the Caldicott Guardian.

4.3 Personal Health & Safety Applicable to Agile Working

The following legislation is applicable to agile working as well as for working in a regular work situation:

- The Management of Health & Safety at Work Regulations 1999: requires employers/employees to assess risks to their health and safety by ensuring that all reasonable controls are put in place to enable safe working.
- The Display Screen Equipment Regulations 1992: do not advocate the use of mobile equipment due to the inability to achieve an ergonomic layout; therefore the use of mobile devices should be minimised to short and infrequent throughout the working day.

The Manual Handling Operations Regulations 1992: should be borne in mind whilst carrying/moving/using the equipment so as to ensure sensible posture is achieved rather than repetitive awkward postures that may culminate in pain/discomfort. To achieve compliance the following actions can be undertaken when moving equipment:

- Use a carrying aid ie. use the case that has been specifically designed to distribute the weight of the mobile device to reduce strain on the body.
- Only carry essential items.
- Reduce the distance of carrying items i.e. parking as close a possible to the given location.

All lifting and handling will be done in compliance with the Moving and Handling Policy.

Whilst agile working, staff should still ensure that all requirements of the Health and Safety Policy are maintained.

Mobile devices are a prime target for theft because they are a valuable item that can be easily snatched. In addition any documentation also needs to be protected for theft or loss. The following actions although not exhaustive should be considered.

Where possible, location should be well lit and adequate parking arrangements made wherever possible.

Valuable equipment should be hidden from view to prevent advertising valuable equipment to thieves.

Staff should report suspicious activity and notify incidents to their line manager so that other staff are aware.

Computers and documentation containing personal or sensitive information should be carried in the locked boot of a car not on the seat of the car from where it can be snatched.

Journeys should be direct from the work location to the place of agile working. Stops should not be made at supermarkets etc whilst carrying such assets or documentation.

Lock the doors on the car to ensure security when stopping temporarily at traffic lights.

Do not leave computers, removable media or sensitive documentation in the car overnight, even if it is in a garage.

Avoid heavy jolts during transit which may render the system inoperative.

Only retrieve, use or carry as much data as you actually need. The more files or records (electronic or manual) the greater the risk of something falling into the wrong hands

4.4 Securing the Data and Computers in the Home

Having ensured that the data and mobile media or device have arrived in the location in which they are going to be used, there is now a need to ensure the sensitive data remains secure and not seen by others who may live in the house.

All health and safety aspects of the working environment must also be complied with.

In addition the use of sensitive or personally identifiable data must be controlled in such a way that approval must be given for its “off site” use. A casual approach to its removal is no longer acceptable, even when it is encrypted.

The following guidelines identify what is, and what isn’t acceptable in respect of using data in a location other than your normal place of work:

- A basic principle across the CCG is that no PCD will be taken off site for any other purpose than the treatment of patients or because meetings requiring access to specific personal data are taking place.
- As a further principle, any PCD taken off site for specific purposes identified above will be returned the same day to the secure work location, where it will be locked away.
- It is recognised that for the CCG and many of its staff to operate efficiently, it is necessary for PCD to be taken home so that meetings external to the CCG can be attended in the early morning or in the late afternoon, when it would be very

inconvenient to return to the work environment. Under these circumstances, the person taking the PCD off site should notify their manager as to what is being removed, for how long and for what reason.

- Users of PCD should have available an email from their manager agreeing to the use of that PCD for agile working.
- Accessing of PCD through the use of a computer linked to the network is as easy as accessing the information in a work environment, but again the user must have emailed agreement for the use of that information. Logs of user's time on the network will identify potential problem areas if data is lost.
- There are some basic principles which apply to agile working whether the information being used is sensitive or not.
- Do not allow any other person to use or play with the computer regardless of whether it is logged in or not.
- Ensure others do not read the content of the screen.
- Do not allow others to read through any documentation which you may be using.
- Log off or lock the mobile device when not using it.
- Do not leave papers lying around. Tidy them away (and store somewhere safely if overnight).
- Do not share passwords with anyone else.
- Dispose of information safely when agile working making sure that confidentiality is maintained. If possible shred any sensitive papers in line with the CCG policy when no longer required or return them to be disposed of in line with CCG policy.
- Be careful when having telephone conversations with colleagues about work whilst agile working, that the conversation cannot be overheard.

4.5 Reporting Security Incidents & Weaknesses

Reporting of any losses, theft or damage to documentation or mobile device assets will be reported through the Incident Reporting System at the first possible opportunity, and with a degree of urgency.

Information provided will include details of the losses or incidents and a detailed description of the data lost. Any PCD lost will need to be reported via the Information Governance Incident Reporting Tool and individual subjects will need to be notified of the losses. Please refer to the Incident Reporting Policy.

Near misses and possible weaknesses should also be reported through the Incident Reporting System.

4.6 Mobile Device Eligibility

Job Role	Desktop/Laptop	Mobile	VPN/3G
Director	Both	Smart phone	Y
Clinical Director	Both	Smart phone	Y
Associate/Deputy	Both	Smart phone	Y

Head/Lead	User preference - based on best fit for function	Smart phone	As appropriate to the job function
Manager	User preference - based on best fit for function	Smart phone	As appropriate to the job function
Other staff	Desktop	N/A unless required for role. To be agreed by relevant AD	N/A unless required for role. To be agreed by relevant AD

This identifies staff cohorts, based on function/role, and what is expected to be the standard offering to them.

The allocation of mobile devices will be at the discretion of the staff member's line manager. All Directors will be given a choice of mobile device to allow them to select what best suits the requirement of their role.

All Directors will be offered the flexibility to use any of the mobile devices within the device catalogue in order to suit their personal requirements as best possible. It is expected that they will use both a desktop and a mobile device, to allow for work to be completed when away from the office which may require office like functionality. However, the CCG is keen to maintain an appropriate mobile device to user ratio so the availability of both desktop and mobile device will be at the discretion of the appropriate Director.

If you require any piece of equipment including mobile devices please log a request with the GMSS IT Service Desk through the Service Now portal (https://nwcsu.service-now.com). They will ask you to complete form with all the relevant information including budget code. The completed price book should be sent to BOLCCG.ITApprovals@nhs.net for consideration.

5 Monitoring and Review

This policy/procedure will be monitored through staff awareness and supporting evidence to the NHS IG Toolkit.

This Policy will be reviewed on an annual basis, 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.

6 References

- Data Protection Act 1998
- Freedom of Information Act 2000

- Information Security Management Systems (ISO:27001:2005)
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 1998
- Freedom of Information Act 2000

- Information Security Management Systems (ISO:27001:2005)
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000

Appendix B - Definitions

IAA – Information Asset Administrator

IAO – Information Asset Owner

Agile Working – This refers to the moving around of information on a mobile device and/or hard copy because this is necessary in order to carry out one's function effectively and efficiently.

PID – Personally Identifiable Data

PCD – Personal Confidential Data

Agile Access - This refers to any technology that enables users to connect securely in geographically dispersed locations and supports mobile working i.e. normal place of work and including working from home. This access is typically over some kind of dial-up connection, broadband or 3G link through a terminal server. This gives the effect of working directly onto the network in the workplace and depending upon what access rights are given, access to emails, files and SharePoint can be made. For email the possibility of using web mail is available.

Agile working - Accessing the CCG's information systems from other than one's normal place of work, including home, possibly taking hard copy material outside of the CCG's premises in order to do so - because this is necessary in order to carry out one's function effectively and efficiently and continued success of the CCG.

SIRO – Senior Information Risk Owner