NHS
Vale of York
Clinical Commissioning Group

MOBILE WORKING POLICY

November 2017

Authorship :	Chris Wallace, Information Governance Manager, North, Yorkshire & Humber Commissioning Support Unit
Reviewing Committee :	Emergency Planning, Business Continuity and Information Governance Steering Group
Date :	Circulated October 2017
Approval Body :	Executive Committee
Approved Date :	15 November 2017
Review Date :	September 2019
Equality Impact Assessment :	Completed
Sustainability Impact Assessment :	Completed
Related Policies :	IG01 Confidentiality Audit Policy IG02 Data Protection and Confidentiality Policy IG03 Internet, Email and Acceptable Use Policy IG04 Freedom of Information Act IG05 Information Security Policy IG06 Information Risk Policy IG07 Corporate Records Management Standards and Procedures IG09 Subject Access Request Policy IG10 Safe Haven Policy IG11 Information Governance Strategy IG12 Clinical Records Keeping Policy and Standards
Target Audience :	All NHS Vale of York CCG employees and persons working for the CCG; all members attending CCG committees and members of the governing body. All contractors providing services to the CCG.
Policy Reference No. :	IG08
Version Number :	3.0

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 and Date	Date on Internet
0.2	Chris Wallace	First draft for	NR	
1.0	P Furneaux, Policy & Assurance Manager	CCG specific amendments	Management Team	
1.1	M Skelton, Business Support Manager	CCG specific amendments	Management Team	
2.0	M Skelton, Business Support Manager	Guidance on appropriate use of corporate devices	SMT February 2016	
2.1 3.0	M Hughes, Business Support Manager	Amendment to Policy relating to Mobile Workers, requesting remote access and identifying labels Reference GDPR Legislation Amendment to reflect Accountable Officer SIRO and Caldicott Guardian and Business Support Manager roles and Data Protection Officer Role	Executive Committee 15/11/2017 Audit Committee 30/11/2017	December 2017

To request this document in a different language or in a different format, please contact the CCG :

01904 555870 or valeofyork.contactus@nhs.net

CONTENTS

1. INTRODUCTION

1.1. Mobile Working is a form of organising / performing work, using information technology, where work, which could also be performed at the employer's premises, is carried out away from those premises on a regular basis. The essential feature is the use of information and communication technologies to enable remote working from the office where people work from home for all or part of their hours with a computer or telecommunication link to their organisation.

1.2. The use of portable computing and telephone devices and the accessing of information from a variety of remote locations is now commonplace within the NHS.

1.3. The Vale of York Clinical Commissioning Group supports flexible working practices and recognises that that there are occasions when the ability to work away from the office is a necessity and/or supports achievement of work / life balance.

1.4. eMBED provide IMT services under a Service Level Agreement (SLA) which include the provision of support for mobile working.

2. POLICY AIM

2.1. The aims of this policy are :

- To ensure that the organisation complies with its legal obligations.
- To promote the safe and secure use of mobile equipment in support of the clinical and operational work of the organisation.
- To provide a secure working practice for personnel working from home.
- To ensure that ICT resources provided to staff are not misused.
- To ensure that the security of computer systems and the information they contain is not compromised in any way.
- To prevent the organisation's reputation from being damaged by the inappropriate or improper use of its information resources.

2.2. The policy applies to all full-time and part-time employees of NHS Vale of York CCG, non-executive directors, governors, contracted third parties (including agency staff), students/trainees, bank staff, staff on secondment and other staff on placement within the organisation, volunteers and staff of partner organisations with approved access. It applies to all areas in support of the business objectives both clinical and corporate.

3. ENGAGEMENT

3.1. This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

4. IMPACT ANALYSES

Equality

4.1. An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

4.2. As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

Sustainability

4.3. A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

5. SCOPE

5.1. This policy applies to all CCG staff and contractors that 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.

5.2. Such equipment includes, but is not limited to:

- Laptop computers
- Tablets
- Smartphones

6. RESPONSIBILITIES

Accountable Officer

6.1. The Accountable Officer has overall responsibility for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Ensure that NHS Vale of York CCG has robust policies and procedures in place to ensure security of information held at all times.

Senior Information Risk Owner, (SIRO)

6.2. The SIRO is the Executive with overall responsibility for information as a strategies asset and for ensuring that the value of information is recognised and understood within the organisation; appropriate Information Governance measures are in place to protect against risk and that appropriate assurance mechanisms exist. The SIRO is

responsible for providing written advice to the Accounting Officer on the content of their annual governance statement in regard to information risk. The SIRO should be satisfied that appropriate measures are in place to protect all mobile devices used for CCG business purposes; and that policies and procedures are in place and communicated to staff to ensure they understand their responsibilities to protect and use mobile devices correctly

Caldicott Guardian, (CG)

6.3. The Caldicott Guardian is a senior person with delegated responsibility for protecting the confidentiality of a patient and service-user information and enabling appropriate information-sharing.

Data Protection Officer (Required from 25 May 2018)

6.4. From May 2018 the General Data Protection Requirement (GDPR) makes it a mandatory requirement for all public bodies to appoint a Data Protection Officer who will be the cornerstone of accountability for Data Protection, facilitate compliance, inform the data controller and the organisation of their obligations, promote a data protection culture and monitor compliance with GDPR. This role must be

- Easily accessible – contact details to be available to data subjects and the Information commissioner's office (ICO)
- Have integrity and high professional ethics
- Be involved properly and in a timely manner in all issues relating to protection of personal data
- Be consulted when a data breach or incident occurs
- Be able to perform duties and tasks in an independent manner, must not be instructed, must be autonomous
- There should be no unfair termination of contract

Business Support Manager, (BSM)

6.5. The CCG's Business Support Manager is the first point of contact for eMBED IT Services regarding management of the CCG's laptop assets. The BSM will verify the CCG's mobile assets register for which eMBED provide support services.

6.6. The CCG has also purchased a number of mobile phones, laptops and tablets for staff use. For the CCG owned and managed mobile devices the BSM is responsible for maintaining the CCG's Mobile Asset Register and providing first line advice. The BSM also the system administrator for these devices and is responsible for configuring, implementing and maintaining device security profiles.

6.7. The BSM is responsible for maintaining records of issue/return of equipment and for ensuring that devices are appropriately sanitised before re-issue/disposal.

Line Managers

6.8. Managers should ensure that personnel allocated mobile IT equipment have a genuine need for mobile computing and that if authorised to work at home, all other staff regulations are met e.g. Health and Safety requirements.

6.9. Managers must ensure that all equipment allocated for mobile working is encrypted to the NHS standard and that all their staff have access to a network drive or other secure backup devices to backup and store confidential information.

All Staff

6.10. All staff allocated mobile computing equipment are expected to take all reasonable measures to safeguard the equipment and are to ensure that its use is in accordance with this policy.

6.11. Staff must ensure that the mobile equipment they use is encrypted to the NHS standard and that all information stored on this equipment is backed up appropriately before becoming mobile. If staff are unsure they must seek support and assurance from the IT Helpdesk.

7. EQUIPMENT PROVIDED TO STAFF

All Staff

7.1. All new starters on via a request from the Line Manager to the Business Support Manager will be provided with appropriate access to IT network and systems and provided with an NHSMail account.

7.2. Some workers will work only from base. The following equipment will be provided :

- Use of Fixed Phone on Desk.
- Use of Fixed Desktop Computer, or laptop which can sit in a docking station on the desk.

Mobile Workers

7.3. Mobile working presents a very real risk to the security and integrity of the CCG's information. The CCG is responsible for information held and managed by the organisation and is potentially liable for any breach or failing in security. There are inherent risks in accessing or transferring personal/ confidential information via mobile devices, this can be data held on laptops, contact details on a mobile phone, or information e-mailed to a home PC. Staff need to be aware of their responsibilities by recognising that risks exist, and by implementing appropriate controls to minimise risk.

7.4. Mobile workers will have the ability to effectively work from a range of business, home or public locations where Wi-Fi is available.

7.5. Equipment provided to mobile workers will comprise:

- Smart phone

- Laptop computer with standard carry case
- External network access via VPN Token

7.6. The current agreement from the Senior Management Team is as follows, kit can be issued relating needs of the business to ensure effective working.

7.7. Smart Phones, VPN tokens or laptops can be issued to all staff that are authorised by the relevant Head of Department to work from home. This may require approval in line with the Flexible Working policy or require to undertake project work and require to work or be contacted remotely.

7.8. If equipment is requested, an email will need to be sent to the Business Support Manager from the relevant Head of Department for action.

Staff Responsibilities of Portal Devices

7.9. Each staff member should have a signed a confidentiality clause as part of their contract of employment. This makes clear that all personal information must be treated carefully and must not be disclosed to unauthorised persons. Within the management of CCG assets especially portable devices each staff member will be asked to sign for receipt of the portable device, and to acknowledge that they have read, understood and will comply with this policy (Appendix C)

7.10. The use of corporate phones and tablets for personal use is not acceptable except for emergency circumstances. This includes downloading personal apps for use on corporate devices and using the devices to store personal data. The CCG is not responsible for any loss of personal data held on the phone if the device was to be wiped. Personal devices are deemed unsecure for work purposes, as some personal devices are smartphones. Android devices have a pre-installed app which is called ‘downloads’ which stores all downloaded attachments and iPhones have an app called ‘iBooks’. If nhs.mail was installed on a personal device, if an attachment was to be opened especially any PDF documents, these would be saved to these applications.

7.11. If a corporate device is issued to a member of staff, then this is intended for exclusive use of the member of staff to whom it has been issued. It should not be loaned or shared with anyone else including other members of staff. The use of all devices will be monitored and any misuse could result in disciplinary action. The SIM card issued with the devices must only be used corporate devices and must not be used with personally owned

8. REQUESTING REMOTE ACCESS

8.1. 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 is required to be sent via email to the Business Support Manager from the relevant Head of Department for action.

9. GUIDELINES

Health and Safety

9.1. 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 are safe etc. It is the employee's duty to always consider the risks surrounding their working environment, and take steps where appropriate.

Theft

9.2. 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 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
- An individual carrying what is clearly a laptop bag is a prime target, so wherever possible ensure you are aware of the risks surrounding you. The use of rucksacks or other non-obvious bags to carry a laptop may be advisable in some circumstances

Privacy and Information Governance

9.3. 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.

9.4. 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 your shoulder. 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. Privacy screens are available on request from the IMT Department . 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.

9.5. 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
- Other operational or reputational damage

Use of Non NHS Computers

9.6. Great care should be taken using publicly-available equipment, such as an Internet café or hotel PC.

- Ensure that controls exist such that access is controlled. Avoid 'free use' facilities where someone can just walk up and use a device. Most Internet cafés have systems which issue a 'one time' password, which allows access only for a prescribed period of time. If this is the case, also ensure you have allowed sufficient time at the end of your period for 'clearing down' any information you may leave behind.
- If you have any doubts that the device is not properly secured (e.g. does not appear to have any anti-virus software installed), then do not use such equipment
- Facilities will be limited when using public equipment, generally to using Outlook Web Access for reviewing and sending emails
- When you have finished, before closing Internet Explorer make sure you clear the browsing history (depending on the version of Explorer, generally, Tools->Internet Options->Clear History), and also remove temporary files (generally Tools->Internet Options->Delete Files). Ensure that the 'Delete All Offline Content' box is ticked.

Storage of Data

- You should never store any data on a non-eMBED supplied device. This applies to home PCs or PCs used in hotels or Internet cafes
- Do not store data on diskette, CD or other similar storage device

Memory Sticks

- If data does need to be stored, then use ONLY eMBED supplied encrypted memory stick. These are available by request from the IMT department, subject to a manager's approval.
- Each encrypted memory stick has a unique serial number and password. Information 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. Memory sticks used to hold and transfer Personal confidential or commercially confidential information should not be shared.

- Memory sticks should not be labelled with any sort of NHS identification. They are secure, and without the password they are useless. It should not be possible to determine that the memory stick is the property of the NHS.

Data and Device Encryption

- All mobile devices MUST be equipped with encryption software
- Laptops supplied by the eMBED will have this pre-installed
- Other devices, such as Smartphones should also be encrypted. Any device supplied by the IMT 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 Business Support Manager in the first instance then the IMT Service Desk if necessary. As a guide an encrypted device will require a password at power-on, whereas an unencrypted one will not. Where a device is required for work purposes it should be obtained through the Business Support who will log the request with the IMT Service desk to ensure it is properly encrypted before being put into use.

Identifying Labels

9.7. All issued Remote devices will have an identifying label which immediately indicate they are NHS property. It is considered good practice for users to 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.

Confidentiality

9.8. 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 standards. Staff should also ensure that they are meeting the requirements of the Data Protection Legislation, and at all times behave in accordance with UK law.

9.9. 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 Trust policies.

10. ACCESSING EMAIL FROM NON-NHS DEVICES

10.1. When accessing your NHSmail account from a non-NHS device (i.e. a home computer, personally owned laptop or in an internet cafe) you should only access the service via the web at www.nhs.net and not through an email programme such as Microsoft Outlook unless you have explicit permission from the organisation to do so.

10.2. Selecting the ‘public’ option means you will only be able to view Microsoft Office or Adobe PDF attachments online. It will not be possible to download any attachments on a ‘public’ session.

10.3. Choosing ‘private’ means you are responsible for the security of any documents you download, as when you open a document it leaves a copy on the PC that others may find.

11. INCIDENT REPORTING

11.1. 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.

11.2. Loss or theft of equipment should be reported to the IMT Service Desk immediately. This will ensure that steps can be taken to prevent the equipment being used on the eMBED hosted network, and in some cases allow the equipment to be disabled remotely.

12. RELATED POLICIES

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

- IG02 Data Protection and Confidentiality Policy
- IG05 Information Security Policy
- IG03 Email, Internet and Acceptable Use Policy

13. FOR MORE INFORMATION CONTACT

The Governance Team
VOYCCG.Governance@nhs.net
NHS Vale of York Clinical Commissioning Group
West Offices
Station Rise
York, YO1 6GA

14. APPENDIX 1 : EQUALITY IMPACT ANALYSIS FORM

1.	**Title of policy/ programme/ service being analysed**
	Mobile Working Policy
2.	**Please state the aims and objectives of this work.**
	The Vale of York Clinical Commissioning Group supports flexible working practices and recognises that that there are occasions when the ability to work away from the office is a necessity and/or supports achievement of work/life balance. The aims of this policy are to ensure that the organisation complies with its legal obligations and promote the safe and secure use of mobile equipment in support of the clinical and operational work of the organisation.
3.	**Who is likely to be affected? (e.g. staff, patients, service users)**
	Staff need to comply with the principles and practices outlined in this policy.
4.	**What sources of equality information have you used to inform your piece of work?**
	NHS England guidance
5.	**What steps have been taken ensure that the organisation has paid due regard to the need to eliminate discrimination, advance equal opportunities and foster good relations between people with protected characteristics**
	The analysis of equalities is embedded within the CCG's Committee Terms of Reference and project management framework.
6.	**Who have you involved in the development of this piece of work?**
	Internal involvement: Senior Management team **Stakeholder involvement**: Consultation with Senior Managers **Patient / carer / public involvement**: This is an Internal policy aimed at staff employed by the CCG and contractors working for the CCG. The focus is on compliance with statutory duties and NHS mandated principles and practice. There are no particular equality implications.

7.	**What evidence do you have of any potential adverse or positive impact on groups with protected characteristics?** **Do you have any gaps in information?** **Include any supporting evidence e.g. research, data or feedback from engagement activities** **(Refer to** Error! Reference source not found. if your piece of work relates to commissioning activity to gather the evidence during all stages of the commissioning cycle)
Disability People who are learning disabled, physically disabled, people with mental illness, sensory loss and long term chronic conditions such as diabetes, HIV)	Consider building access, communication requirements, making reasonable adjustments for individuals etc.
N/A	
Sex Men and Women	Consider gender preference in key worker, single sex accommodation etc.
N/A	
Race or nationality People of different ethnic backgrounds, including Roma Gypsies and Travelers	Consider cultural traditions, food requirements, communication styles, language needs etc.
N/A	
Age This applies to all age groups. This can include safeguarding, consent and child welfare	Consider access to services or employment based on need/merit not age, effective communication strategies etc.
N/A	
Trans People who have undergone gender reassignment (sex change) and those who identify as trans	Consider privacy of data, harassment, access to unisex toilets & bathing areas etc.
N/A	

Sexual orientation This will include lesbian, gay and bi-sexual people as well as heterosexual people.	Consider whether the service acknowledges same sex partners as next of kin, harassment, inclusive language etc.
N/A	
Religion or belief Includes religions, beliefs or no religion or belief	Consider holiday scheduling, appointment timing, dietary considerations, prayer space etc.
N/A	
Marriage and Civil Partnership Refers to legally recognised partnerships (employment policies only)	Consider whether civil partners are included in benefit and leave policies etc.
N/A	
Pregnancy and maternity Refers to the pregnancy period and the first year after birth	Consider impact on working arrangements, part-time working, infant caring responsibilities etc.
N/A	
Carers This relates to general caring responsibilities for someone of any age.	Consider impact on part-time working, shift-patterns, options for flexi working etc.
N/A	
Other disadvantaged groups This relates to groups experiencing health inequalities such as people living in deprived areas, new migrants, people who are homeless, ex-offenders, people with HIV.	Consider ease of access, location of service, historic take-up of service etc.
N/A	

8.	**Action planning for improvement** Please outline what mitigating actions have been considered to eliminate any adverse impact? No adverse equality impact has been identified. Please state if there are any opportunities to advance equality of opportunity and/ foster good relationships between different groups of people? An Equality Action Plan template is appended to assist in meeting the requirements of the general duty

Sign off
Name and signature of person / team who carried out this analysis *Governance Team*
Date analysis completed *15th September 2017*
Name and signature of responsible Director
Date analysis was approved by responsible Director

16. APPENDIX 2 : SUSTAINABILITY IMPACT ASSESSMENT

Staff preparing a policy, Governing Body (or Sub-Committee) report, service development plan or project are required to complete a Sustainability Impact Assessment (SIA). The purpose of this SIA is to record any positive or negative impacts that this is likely to have on sustainability.

Title of the document	Management of Conflict of Interests Policy
What is the main purpose of the document	The Vale of York Clinical Commissioning Group recognises that conflicts of interest are unavoidable and therefore has in place arrangements to seek to manage them. The measures outlined in this policy are aimed at ensuring that decisions made by the CCG will be taken, and seen to be taken, uninfluenced by external or private interests.
Date completed	15th September 2017
Completed by	P Furneaux, Risk and Assurance Manager

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = N/A	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced?
Travel	Will it provide / improve / promote alternatives to car based transport?	0		
	Will it support more efficient use of cars (car sharing, low emission vehicles, environmentally friendly fuels and technologies)?	0		
	Will it reduce 'care miles' (telecare, care closer) to home?	0		
	Will it promote active travel (cycling, walking)?	0		
	Will it improve access to opportunities and facilities for all groups?	0		

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = N/A	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced?
	Will it specify social, economic and environmental outcomes to be accounted for in procurement and delivery?	0		
Procurement	Will it stimulate innovation among providers of services related to the delivery of the organisations' social, economic and environmental objectives?	0		
	Will it promote ethical purchasing of goods or services?	0		
Procurement	Will it promote greater efficiency of resource use?	0		
	Will it obtain maximum value from pharmaceuticals and technologies (medicines management, prescribing, and supply chain)?	0		
	Will it support local or regional supply chains?	0		
	Will it promote access to local services (care closer to home)?	0		
	Will it make current activities more efficient or alter service delivery models	0		
Facilities Management	Will it reduce the amount of waste produced or increase the amount of waste recycled? Will it reduce water consumption?	0		
Workforce	Will it provide employment opportunities for local people?	0		
	Will it promote or support equal employment opportunities?	0		

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = N/A	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced?
	Will it promote healthy working lives (including health and safety at work, work-life/home-life balance and family friendly policies)?	0		
	Will it offer employment opportunities to disadvantaged groups?	0		
Community Engagement	Will it promote health and sustainable development?	0		
	Have you sought the views of our communities in relation to the impact on sustainable development for this activity?	N/A		
Buildings	Will it improve the resource efficiency of new or refurbished buildings (water, energy, density, use of existing buildings, designing for a longer lifespan)?	0		
	Will it increase safety and security in new buildings and developments?	0		
	Will it reduce greenhouse gas emissions from transport (choice of mode of transport, reducing need to travel)?	0		
	Will it provide sympathetic and appropriate landscaping around new development?	0		
	Will it improve access to the built environment?	0		

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = N/A	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced?
Adaptation to Climate Change	Will it support the plan for the likely effects of climate change (e.g. identifying vulnerable groups; contingency planning for flood, heat wave and other weather extremes)?	0		
Models of Care	Will it minimise 'care miles' making better use of new technologies such as telecare and telehealth, delivering care in settings closer to people's homes?	0		
	Will it promote prevention and self-management?	0		
	Will it provide evidence-based, personalised care that achieves the best possible outcomes with the resources available?	0		
	Will it deliver integrated care, that co-ordinate different elements of care more effectively and remove duplication and redundancy from care pathways?	0		

17. APPENDIX C : FREQUENTLY ASKED QUESTIONS

What is an Authentication Token ?

An Authentication token is a small device that is associated with your personal network login account. When you are issued a token you will be required to enter a personal identification number (PIN) upon its first use. When the token is used in conjunction with your network login and password for remote access to the network, you are only given access if the following details are entered correctly:-

- Your Personal Login Name or Username (this is the same login name you use to access the network when at Trust premises)
- Your Personal Password
- Your Token Pin
- The Secure Token rolling Number

18. APPENDIX D : GUIDANCE WHILE WORKING REMOTELY

All staff

- 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.
- 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 the 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.
- Users are responsible for their authentication token and the associated PIN. You must never tell anyone your PIN. If you suspect someone knows your PIN you must inform IMT Service Desk immediately in order to have the token disabled.
- Users are responsible for any loss of their authentication token. If you lose your authentication token you must report this to IMT service Desk immediately.
- You or your department are responsible for any costs associated with lost or stolen authentication tokens.
- Equipment should **never** be left in vehicles overnight.

19. APPENDIX E : ISSUE OF LAPTOP / MOBILE DEVICE

Name:	
Job Title:	
Site:	
Line Manager & Directorate:	
Contact Telephone:	
	Date Issued:
Please Tick If You Use	
Laptop (specify make, model & serial no) • Laptop carry case	
• Mouse	
• USB Pens/Drives	
VPN Token (specify serial no)	
iPhone (please specify if this is mobile & data) • Mobile phone (please specify number)	
• SIM Number	
• IEMI Number	

This form must be completed by all staff using portable equipment, including personally owned Devices when accessing the network remotely using VPN Token.

I confirm that I have received a portable device and have read, understood and will comply with the Mobile Working Policy.

Print Name:	Signature:	Date:
Manager:		