IG.36 Mobile Working (Remote Access) Policy

Document Number	IG.36 V3.1
Date Ratified	14.06.2019
Date Implemented	28.02.2015
Next Review Date	06.06.2022
Accountable Director	Director of Resources
Policy Author	Information Governance / Privacy Officer

Important Note:
The Intranet version of this document 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.

After the Review Date has expired, this document may not be up-to-date. Please contact the document owner to check the status after the Review Date shown above.

If you would like help to understand this document, or would like it in another format or language, please contact the document owner.

Table of Contents

1. Scope

This policy is applicable to all Trust staff, voluntary, private, third party, agency or sub-contractors working for / on behalf of the Trust, who at any time process information using mobile working/teleworking practices when:

- handling hard copy records away from their normal place of work
- accessing the Trust's IT network from home or from connections outside of the office/Trust environment.

2. Introduction

Mobile working and the use of mobile devices to gain remote access to NHS information assets is becoming common place. The security of mobile devices and hardcopy documentation when used away from the normal place of work must be maintained by staff to ensure that information assets are protected.

Trust staff need to be aware of mobile working/teleworking security issues i.e. the physical security of mobile devices, confidentiality considerations in relation to manual and electronic records, and implications for the security of the Trust's systems and networks.

Staff may only use non NHS owned equipment for work related activities if the equipment and the use of the equipment has been approved.

3. Statement of Intent

This policy has been developed to promote good information security practices when staff undertake mobile working/teleworking, and working in public areas.

4. Definitions

4.1 Mobile Working

Is where staff work away from their normal place of work i.e. in the community or at home using mobile devices or hardcopy documentation.

4.2 Teleworking

Is the use of communication technology to enable staff to work remotely from a fixed location outside of the Trust (including working in the Community or at home).

4.3 Mobile Devices

This includes any device that can store data and can be managed by the IT provider. Typically Laptops, tablet computers, Mobile Phones etc . (PDA's).

4.4 Storage Devices

This includes devices which are able to store data but cannot be managed by the IT provider. Typically MP3 players, digital cameras and visual recording/playback devices.

4.5 Mobile Computing

The use of a Trust Mobile Data Device in any location and/or the processing of that Trust information e.g. a member of staff using a Trust laptop on a train to process their Trust emails.

4.6 Media

Any physical item that can store information and requires another device to access it. For example: CD/DVD's, tapes, digital storage device (flash memory cards, USB discs / memory sticks & portable hard drives).

4.7 BYOD (Bring Your Own Device) – Using a personal (Non-work) mobile device (Smartphone or Tablet) for business purposes.

4.8 MDM (Mobile Device Management) – Software that provides a secure environment for using mobile devices. This software will allow access to your Trust account emails and calendars.

4.9 Encryption – The conversion of data into a form which cannot be easily understood by an unauthorised person.

4.10 Unsecured public Wi-Fi Network – A public Wi-Fi network where you are not required to enter a password to gain access.

4.11 Data

4.11.1 **Personal Data** is classified as any data which enables an individual to be identified from that data as defined in the Data Protection Act 2018. This type of information should be handled with care and not inappropriately disclosed to others i.e. a patients name and address.

4.11.2 **Sensitive Personal Data** is classified as sensitive information under the Data Protection Act 2018. This type of information should be handled with care and not inappropriately disclosed to others i.e. Healthcare Information.

4.12 Information Assets

Information assets include information printed / written on paper, digital images, or information spoken in conversation, as well as information stored electronically on servers, web sites, intranets, PC's, laptops, mobile phones and PDA's as well as on CD ROMs, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically and in the post.

4.13 Contracts and NDA's

4.13.1 **Contracts:** Contractual arrangements with third parties must include agreement on confidentiality control and how this is to be applied. Where confidential information is to be (or could be) accessed the Trust will require the third party to have formal contractual confidentiality clauses with all employees accessing such data.

4.13.2 **Non-Disclosure Agreement (NDA):** where no contract exists staff must ensure that a valid NDA agreement is in place before access to information is allowed.

5. Duties

5.1 **Staff working for or on behalf of the Trust –** are expected to adhere to this policy when undertaking mobile working/teleworking or when remotely accessing the Trusts IT network, systems or software. Staff shall implement the Trusts information governance policies and practices and ensure confidentiality, integrity and data availability is maintained.

5.2 **The IT Provider –** is responsible for adhering to the Trusts policies and procedures with regard to the management of mobile devices.

5.3 **The Data Protection Officer / Head of Information Governance and Data Quality –** Is responsible for approving or declining a Bring Your Own Device (BYOD) request together with overall responsibility for monitoring this policy.

5.4 **All Managers/Departmental Heads –** Are responsible for ensuring that staff who undertake mobile working/teleworking and those who have remote access abide by this policy.

6. Mobile Working/ Teleworking and Remote Access

Mobile working/teleworking and remote access can take place both within and outside Trust premises.

6.1 Staff Responsibilities

Trust staff should be aware that carrying or using mobile devices in public places is likely to draw attention to them and may increase the risk of theft and unauthorised disclosure of information.

Staff who adopt mobile working / teleworking practices need to follow the guidance provided in this policy.

If a member of staff requires remote access to the Trusts Network i.e. to view emails or update an IT system etc. please refer to policy IG 14 and complete the Network Access/Amendment Form.

If a member of staff is aware of an incident where data has been lost or disclosed etc. they must immediately log an incident on Datix, inform their line manager and inform the Information Governance Team. I.e. if a mobile device has been lost Staff will be asked to provide details of the make, model, Asset Number and the content/details of what was lost. If hard copy records are lost they will be asked to provide details about the types of records lost and details of the patients affected.

Staff must ensure that:

6.1.2 They do not access/use/store the Trust's personal, sensitive or company confidential data at home, use mobile devices and/or remote access facilities unless express approval has been given by their line manager and this has been documented in an authorisation email6.1.3 If using mobile devices and remote access facilities they must complete and pass their annual Information Governance Training.

6.1.4 Information assets, when not in use, are locked away. If the asset is stored on Trust premises, access should only be available to authorised members of staff.

6.1.5 Mobile devices or paper based information are never left unattended in public areas.

6.1.6 Mobile devices and information assets are transported (in a clean environment) out of public sight i.e. in the boot of a car and stored securely i.e. in cases, bags, boxes or tamper proof wallets etc.

6.1.7 Information assets are not placed in locations where they could be forgotten, i.e. overhead racks on trains, taxi boots and in exhibition halls etc.

6.1.8 Mobile devices are not used outside of the normal geographical area including outside of the European Economic Area without the permission of the Head of Information Governance and Data Quality.

6.1.9 They take precautions to protect confidential information ensuring that it cannot be seen or overheard by unauthorised individuals whilst working in public areas and work as discreetly as possible.

6.1.10 They prevent unauthorised access to WVT information which is stored within the Mobile Device Management's secure container from relatives /friends/visitors and others.

6.1.11 Any portable device owned by the Trust which has internet connectivity, is used in accordance with the Trust's email policy IG 08 and information security policies IG 19 etc. Wherever devices are used, staff must not access unsuitable material on the internet and refrain from activities which may compromise the Trusts network security.

6.1.12 They are on a secure network connection before mobile devices are used to gain remote access to the Trust's electronic network.

6.1.13 They do not connect their mobile devices to unsecured public Wi-Fi networks.

6.1.14 They do not enable the Bluetooth function on their device whilst using the device for business use unless authorised by the Information Governance team

6.1.15 They do not disable the anti-virus protection software installed on any mobile device.

6.1.16 All removable media devices, such as USB pen drives, are encrypted to the recommended NHS standard before any information is stored on them. They must also virus check all removable media devices before downloading information onto trust equipment or the Trust's network.

6.1.17 Access to mobile devices is restricted to the member of staff or team to who it was issued.

6.1.18 SIM cards are not transferred between different mobile devices; such as laptops, blackberries, mobile phones etc. Should there be a requirement to change the device (with which the SIM card is associated) a job should be logged with the IT Provider's Service Desk.

6.1.19 Their mobile device/s chargers (where applicable) are made available for annual Portable Appliance Testing (PAT).

6.1.20 They do not write down their passwords and keep them with their mobile device/access tokens.

6.1.21 They do not leave their Smartcards in their mobile devices when unattended.

6.1.22 Only the minimum amount of data required is stored on mobile device/s or in paper record format.

6.1.23 **Where possible** only "copy" electronic or paper documentation i.e. patient records are taken "off-site".

6.1.24 They do not save data onto the C:\drive of any laptop.

6.1.25 They notify the IT Providers Service Desk if they believe that their mobile device is not encrypted or protected by mobile device management software and stop using the device immediately.

6.1.26 They do not install or download any unauthorised software/data.

6.1.27 Personal data is removed from any mobile device/s in line with the Trusts policies.

6.1.28 They immediately notify their line Manager and the Information Governance Team if any Trust information is destroyed, damaged or if confidentiality is broken and complete a Datix straight away.

6.1.29 They immediately report Trust lost or stolen mobile devices and or/media to their Line Manager and the Information Governance Team and complete a Datix straight away.

6.1.30 They do not dispose of any media off-site. Waste should be returned to a Trust site and disposed of in an appropriate manner i.e. in a confidential waste bin.

6.1.31 They do not store Personal Data, Sensitive Personal Data or Sensitive Organisational information on IT equipment not owned and managed by the Trust unless this has been approved by following the processes in 6.6 Bring your Own Device (BYOD).

6.1.32 Any personal or sensitive personal data which is sent or received by email on a mobile device is sent via secure mail addresses i.e. NHS.net to NHS.net or from a Trust email account to another Trust email account. If information is sent via another route approval must be sought from the Information Governance Team and the data must be encrypted. If sending over 50 records approval has to be sought from the Caldicott Guardian. For further information see the Information Governance Intranet Page.

6.1.33 They do not send any Trust data to their insecure personal email address i.e. fred.bloggs123@hotmail.co.uk.

6.1.34 They obtain a trust encrypted USB device by contacting the IT Providers Service Desk. Staff are not permitted to store confidential trust information on their own memory sticks.

6.1.35 They do not connect their Mobile Phones, Smart Phones and BlackBerries to a Trust's computer asset for any purpose other than to charge the device.

6.1.36 Seek authorisation to purchase a trust mobile device from their Line Manager.

6.1.37 They are aware of their responsibilities in relation to the capture and use of cameras and digital images for further guidance refer to IG 61 Image/s and Recording/s Policy and Procedure.

6.2 **Managers Responsibilities**

Managers must:-

6.2.1 Risk-assess the option of Mobile working/teleworking and/or remote access on a case by case basis, assessing each member of staff's responsibilities and ability to meet the requirements of this policy.

6.2.2 Approve where appropriate, staff requests for Mobile working/teleworking and/or remote working and confirm approval to the member of staff in a WVT email.

6.2.3 Approve where appropriate, staff requests to use their own devices for work and complete and approve the Bring Your Own Device (BYOD) Consent Form in association with the Head of Information Governance and Data Quality Appendix 1.

6.2.4 Check with staff who undertake Mobile Working /Teleworking and/or remote working the physical security of the environments where it is proposed that Trust information will be processed and stored.

6.2.5 Determine the level of access granted to members of staff for network drives and information systems.

6.2.6 Notify the IT Provider Service Desk when a member of staff no longer requires remote access to the Trust's systems.

6.2.7 Ensure that this policy is read by all staff who undertake Mobile working/teleworking and /or remote access to Trust systems.

6.2.8 Ensure that confidential information is not stored on unencrypted mobile devices.

6.2.9 Ensure that data is removed from approved mobile device/s in a timely manner in line with the Trusts policies.

6.2.10 Ensure that all mobile equipment is returned from staff when they leave or transfer to another role. The manager should log a job with the IT Providers Service Desk so the returned equipment can be collected by the IT Provider to ensure that all data held on the device/s is securely erased. The manager should ensure that the IT Provider completes the IT Equipment Return Form.

6.2.11 Ensure all potential and actual security breaches are reported and investigated in accordance with HS 05 Incident Management Policy and undertaking a root cause analysis where appropriate.

6.2.12 Ensure that when third parties or candidates attend for meetings/interviews they email information through to be virus checked or obtain approval from the Information Governance Team to allow individuals to access the Trusts network.

6.2.13 Ensure that staff undertake and pass their annual Information Governance Training.

6.3 IT Providers Responsibilities

The IT Provider must ensure that:

6.3.1 The allocation of Trust mobile devices is recorded on the Asset Register, naming the member of staff they have been allocated to.

6.3.2 On receipt of update from staff/line manager they update the Asset Register to reflect any change of user/department and/or storage/decommissioning of any mobile computing device or media.

6.3.3 All data stored on redundant mobile devices is removed before the mobile device is put into storage or re-allocated to another user.

6.3.4 All Trust mobile devices i.e. laptops and USB devices are encrypted to the recommended NHS standard before any information is stored on them.

6.3.5 All supplied mobile devices are managed by the corporate mobile device management solution where appropriate.

6.3.6 All mobile devices owned by the Trust are marked with an asset code.

6.3.7 Where appropriate all mobile devices have anti-virus, updated regularly and encrypted where possible in order to prevent the potential for a malicious or unauthorised mobile code attack.

6.3.8 All mobile devices which have access to the Trust's network or systems/software can be remotely wiped of data in the event of the device being lost or stolen.

6.3.9 Remote staff access to networked systems is restricted to the minimum necessary to enable staff to carry out their role via mobile devices i.e. via RAS accounts.

6.3.10 When providing system access to third party contractors their third party status will be identified.

6.3.11 Remote network access for third party suppliers or partner organisations will not be permitted unless approval has been given from the WVT Information Governance Team.

6.3.12 Trust mobile equipment is stored securely whist Kept on the IT Providers premises.

6.3.13 The Trust's network is monitored and the connection of any unauthorised device is detected and prevented according to established NHS and Government standards.

6.3.14 Ensure that when required third parties or candidates can use an encrypted memory device on Trust networked equipment.

6.3.14 Arrangements for equipment containing storage media to be sanitised to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to secure disposal or re-use.

6.4 Trust Responsibilities

The Trust must ensure that:-

6.4.1 Mobile devices (where applicable) are annually Portable Appliance Testing (PAT) tested.

6.4.2 The organisation undertakes regular fraud preventative exercises to detect unsuitable phone usage (for example to review frequently dialled numbers, high cost calls, calls dialled outside normal working hours, calls to premium numbers or foreign countries).

6.5 Bring Your Own Device (BYOD)

6.5.1 Users are not allowed to connect their own personal equipment to the Trust's network due to the threat of security breaches and viruses unless approval has been given by the Head of Information Governance and Data Quality.

6.5.2 The use of personally-owned phones is prohibited for business use with regard to data transfer and storage. Staff must not synchronise their personal phone devices (including iPhones, Smartphones and Blackberry's) with their business Microsoft Outlook as this will result in an unencrypted copy of potentially confidential information being stored on their own device.

6.5.2 Voice calls from a personal phone for business purposes are permitted.

6.5.3 In general the use and storage of Trust personal data, sensitive personal data or confidential corporate information on staff owned equipment is strictly forbidden. Staff are only permitted to use Trust supplied equipment for this purpose. Exceptions to this requirement may be made by the Head of Information Governance and Data Quality and will be assessed on a case by case basis.

6.5.4 Staff who wish to use their own equipment for work must complete the Bring your Own Device (BYOD) Consent form Appendix 1 and return the original to the Information Governance Team for approval. A copy should be kept on the staff's personnel file.

6.5.6 Any existing data stored on the personal mobile device will be wiped before the equipment can be used by the member of staff for Trust purposes i.e. a factory reset so it's in a known state. The Trust's Mobile Device Management application will be loaded onto the device by the Trust's IT Provider and the mobile device will be managed via the mobile working application. All personal data stored on the device will be accessible to the IT Provider.

6.5.7 Access to specific websites shall be controlled by a relevant white or black list. If the user wishes to gain access to a website which they believe should be

granted for business purposes, then they must request this from Information Governance.

6.5.8 In the event that the member of staff no longer wishes to use their personal mobile device for work or if they leave the Trust the IT Provider will remotely wipe all data held on the personal device.

6.5.9 Users of personally owned devices will receive support for connectivity and MDM functions only. Responsibility for the end device support remains with its owner.

6.5.10 No attempt will be made to resolve issues with devices which do not meet the minimum standard. For instance, devices running an older operating system than Android 3.0 or iOS 5.0.

7 Training

There is no mandatory training to directly fulfil this policy, but WVT staff should complete their mandatory annual Information Governance Training. The Mobile Working Information Governance leaflet is available on the Information Governance Intranet Page which provides a summary of the information contained in this policy.

8. Monitoring compliance with this policy

All procedural documents will include a section on how they will be monitored, using the following table. Monitoring of this specific procedural document will be overseen by the Policy Sub Group. See detail in the attached table:

Aspect of compliance or effectiveness being monitored	Monitoring method	Individual responsible for monitoring	Frequency of the monitoring activity	Group/ committee which will receive the findings/ monitoring report	Group/ committee/ individual responsible for ensuring that the actions are completed
Review of Policy to ensure it meets all the current obligations in Law.	The Information Governance / Privacy Officer will review the Policy and report to the Information Governance and Health Records Committee any changes/revisions which are required	Information Governance / Privacy Officer	Annually	Information Governance and Health Records Committee	Information Governance and Health Records Committee
Review of Policy to ensure that all processes, groups, and individuals contained within the Policy are still accurate.	As above	As above	As above	As above	As above
Review of Policy to ensure it stays compliant with the latest best practice guidelines from organisations such as Connecting for Health, the Information Commissioners Office and the National Information Governance Board.	As above	As above	As above	As above	As above
Review of Policy to ensure it meets all the requirements to be used as evidence in the annual Information Governance Toolkit submission.	As above	As above	As above	As above	As above

9. Related Trust Policy/Procedures

- IG.14 User Access Control Policy
- IG.05 Confidentiality Code of Conduct
- IG.12 Data Protection Act Policy
- IG 07 Internet Access Policy
- IG.21 Network Management Policy
- MF.30 Risk Management and Assurance Procedure
- IG 08 E-Mail Access and Use Policy
- IG 16 Physical and Environmental security Policy
- IG 19 IT Equipment and Digital Data Disposal Policy
- IG 17 Systems Back Up and Restore Policy
- IG 61 Image/s and Recording/s Policy and Procedures
- HS 05 Incident Management Policy

10 References

This policy has been written to meet the requirements of:

- Common Law Duty of Confidentiality
- Confidentiality: NHS Code of Practice
- The Data Protection Act 2018
- General Data Protection Regulations 2018
- The Computer Misuse Act 1990

11. Equality Impact Assessments

The Trust recognises the diversity of our staff and community. Our aim is therefore to provide a safe environment free from discrimination and a place where all staff and users of our services are treated fairly, with dignity and appropriately to their need.

In line with the Equality Act 2010 an Equality Impact Assessment was carried out at the developmental stage of this document. No detriment was identified.

1	**Name and Job Title of person completing assessment**	Sarah Roach Information Governance / Privacy Officers
2	**Name of service, policy or function being assessed**	Mobile working (Remote Access) Policy
3	**What are the main objectives or aims of the service/policy/function?**	This policy outlines the procedures and processes required when remote access to the Trust ICT network, systems or software is requested. It also sets down the expectations of staff conduct and use of remote access once it has

		been approved.
4	**Date**	08/10/2014

Stage 1: Initial Screening

5	**What evidence is available to suggest that the proposed service/policy/function could have an impact on people from the protected characteristics? Document reasons, e.g. research, results of consultation, monitoring data and assess relevance as: *Not relevant or Relevant Low/Medium/High***

	Protected Characteristic	Relevance	Evidence
A	Race	***Not relevant***	
B	Religion/Spirituality	***Not relevant***	
C	Gender	***Not relevant***	
D	Disability	***Not relevant***	
E	Sexual Orientation	***Not relevant***	
F	Age	***Not relevant***	
G	Pregnancy/maternity	***Not relevant***	
H	Gender reassignment	***Not relevant***	
I	Marriage and Civil Partnership	***Not relevant***	
J	Carers	***Not relevant***	

If you assess the service/policy/function as **not relevant**, please proceed to section 11.
If you assess the service/policy/function as **relevant**, continue to Stage 2, Full Equality Impact Assessment.

Stage 2: Full Equality Impact Assessment

6	**Are there service user, public or staff concerns that the proposed service/policy/function may be discriminatory, or have an adverse impact on people from the protected characteristics?**	
A	Public	
B	Staff	

If there are **no concerns** proceed to section 11.

If there **are concerns,** amend service/policy/function to mitigate adverse impact, consider actions to eliminate adverse impact, or justify adverse impact

7	**Can the adverse impact be justified**
8	**What changes were made to the service/policy/function as result of information gathering?**
9	**What arrangements will you put in place to monitor impact of the proposed service/policy/function on individuals from the protected characteristics?**
10	**List below actions you will take to address any unjustified impact and promote equality of outcome for individuals from protected characteristics. Consider actions for any procedures, services, training and projects related to the service/policy/function which have the potential to promote equality.**

Action	Lead	Timescales

11	**Review date**	

I am satisfied that this service/policy/function has been successfully equality impact assessed.
Date: 06/06/2019
Author: Sarah Roach Information Governance Officer

Please send the completed assessment for scrutiny to: Risk & Security Support Officer, Vaughan Building, Ruckhall Lane, Belmont, Hereford. HR2 9RP.

Bring Your Own Device (BYOD) Consent Form

Any staff employed by Wye Valley Trust (WVT) wishing to use personally owned mobile devices for work purposes must complete the consent form below.

All healthcare information is classified as sensitive personal information under the Data Protection Act 1 2018 and the Trust has to ensure that this type of information is handled with care and is not inappropriately disclosed to others.

As part of this consent process the following WVT policies must be read and understood by the member of staff signing this form:

IG.05 Confidentiality Code of Conduct	IG 16 Physical and Environmental security Policy
IG 07 Internet Access Policy	IG 17 Systems Back Up and Restore Policy
IG 08 E-Mail Access and Use Policy	IG 21 Network Management Policy
IG 19 IT Equipment and Digital Data Disposal Policy	IG 14 User Access Control Policy
IG.12 Data Protection Act Policy	IG 61 Image/s and Recording/s Policy and Procedure

All staff must also complete mandatory Information Governance Training annually.

"I understand that any data already on the mobile device will be wiped before the WVT Mobile Device Management software is added to the device.

The mobile device will be managed completely via the mobile working application and that any of my personal or home data stored on the device will be accessible by the IT Provider.

In the event that I no longer wish to use my personal mobile device at work or if I leave WVT I understand that the device will be wiped of all data by the IT Provider.

I understand that if the device is lost or stolen an incident must be raised immediately through DATIX, I will inform the Information Governance Team and the device will be remotely wiped of all data by the IT Provider.

I have read and understood all of the required polices as detailed above."

Name (please print)		Signed	
Managers Name) (please print)		Signed	
Date			
Department and Location of work			
Has this request been approved by the Head of Information Governance and Data Quality (circle) Yes No			

The original of this form is to be returned to: Information Governance Team, Monkmoor Court, 31-34 Commercial Road, Hereford, HR1 2BG. Tel: 01432 262077/262078