Lincolnshire Community Health Services
NHS Trust

Mobile Phone and Remote Access Policy

Reference No:	P_IG_31
Version:	1
Ratified by:	LCHS Trust Board
Date ratified:	14 August 2018
Name of originator/author:	Kaz Scott, Information Governance Lead
Name of responsible committee / individual:	Information Governance Management Assurance Group
Date issued:	August 2018
Review date:	August 2020
Target audience:	LCHS staff
Distributed via:	Website

Lincolnshire Community Health Services NHS Trust

Mobile Phone and Remote Access Policy

Version Control Sheet

Version	Section/Para/ Appendix	Version/Description of Amendments	Date	Author/ Amended by
1		Amalgamation of policies (P_IG_03, 05, 23), content previously ratified and further content updated to reflect GDPR.	May 2018	Kaz Scott
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Lincolnshire Community Health Services NHS Trust

Mobile Phone and Remote Access Policy

Contents

Lincolnshire Community Health Services NHS Trust

Mobile Phone and Remote Access Policy

Policy Statement

Background

The Trust recognises that it needs to be in contact with its staff on a regular basis and that some are required to work by themselves for significant periods of time in the community without close or direct supervision, in isolated work areas and often out of normal working hours.

The purpose of this policy is to ensure appropriate communications, both voice and data to protect staff, so far as is reasonably practicable, from the risks of lone working.

This policy conforms to current legislation and other Trust associated policies:

- Data Protection Policy
- Information Security Policy
- Lone Worker and Violence and Aggression at Work Policy
- Disciplinary Policy and Investigation Process
- Incident Reporting Policy
- Agile Working Policy

Statement

The Trust is committed to the management of risk and to improve communications across the Trust.

Responsibilities

Compliance with the policy will be the responsibility of all Trust staff. Managers are responsible for monitoring the application of the policy.

Training

All devices are provided with instruction manuals and any additional advice and training will be given on issue of the devices.

Dissemination

The policy will be available to all Trust staff on the Website.

Resource Implication

Cost of all devices and ongoing rental to be borne by budget holder applicable to the service area / business unit.

MOBILE PHONE AND REMOTE ACCESS

The objectives are:

- To outline the key elements of the Trust's mobile telephone and remote access management arrangements and to detail the responsibilities of managers and staff.
- To improve communication in the Trust in a controlled, accountable manner, offering value for money.

It seeks to ensure that adequate procedures exist for:

- management and use of equipment
- procurement requirements
- security of communication and equipment

Definitions

"Mobile telephone' is defined as a telephone not physically connected to a landline. Cordless telephones which are an extension of a telephone physically connected to a landline are not included.

'Private usage' means telephone calls made (or accepted reverse charge calls), which are not wholly, exclusively and necessary in the performance of the employer's duties.

'Data Card' is defined as remote access hardware.

General Statement

Mobile telephones, Data Card or MiFi will be provided by the Trust for work related purposes at the discretion of the Director/Head of Service.

With prior approval by the Director/Head of Service, mobile phones can be used for private purposes. Private calls will be charged to individuals in line with Inland Revenue requirements.

The mobile telephone or Data Card is at all times the property of the Trust.

Where appropriate, mobile telephones will be used on a pool basis. Pool telephones will not be authorised for private use. Trust mobile phones should not be used when a landline is available unless on an inclusive call tariff.

In certain circumstances staff may be authorised by their Director/Head of Service to use their own private mobile phones for business use and will be able to reclaim call charges via their normal expense claims. Neither hand held nor hands free phones should be used in a car when on Trust Business.

Management Responsibilities

Directors / Heads of Service:

- Responsible for the authorisation of the purchase/rental of mobile telephones, Data Cards or MiFi. Shared usage or mobile telephones, where appropriate is to be adopted and encouraged.
  Any member of staff unhappy to utilise a Trust mobile telephone, due to safety concerns, is not obliged to do so
- On requisitioning a data card for remote access or activation of an integrated data card within a laptop, request associated VPN access by completing the relevant form.
- To notify the ICT Department of any transfers or withdrawals of any devices particularly when a member of staff leaves the Trust.

- To ensure funding is available within the directorate budget to support both costs of purchase, rental and call charges of the equipment.

Arden & GEM CSU ICT Services:

- Responsible for procurement, issue and disposal of Trust mobile telephones, Data Cards and MiFi
- Will ensure all current safety guidelines referring to the operation of mobile telephones, Data Cards and MiFi are made known to staff. Operational procedures will be amended to reflect changes in government advice

Authorisation

The purchase of mobile telephones and MiFi is only to be authorised for:

- Staff who work in isolation, usually in the community providing the purchase of such equipment is supported by a formal risk assessment in line with the Trust's Lone Worker and Violence and Aggression at Work Policy
- Staff who need to be easily contactable during their normal working day due to the nature of their role
- Staff who are regularly on-call or on standby and need to be easily contactable outside of normal working hours. Dependent upon the frequency of this commitment, staff may be required to share equipment
- Staff who need regular off site access to the Trust's computer networks

Procurement Strategy

Arden & GEM CSU ICT Services

- Will process all mobile telephone / MiFi orders upon receipt of an appropriate completed and authorised requisition from the Director / Head of Service
- Will purchase all the Trust's mobile telephones and MiFi using the current contract network provider;
- Will determine the most suitable tariff for connection on information from the requisition details
- Will monitor the use of mobile telephones, Data Cards and MiFi using the network providers monthly call statement and amend any tariffs, as necessary, to the most appropriate for the level of call spend;
- Will report any signs of misuse to the appropriate Director / Head of Service with regards to the unusually high level of call spend or extended call duration;

User's responsibility

All staff provided with a mobile telephone are required to complete Declaration of Use of Mobile Telephone Form'. Where private use has been indicated this includes an agreed monthly deduction from salary to cover the cost of private use.

The user should take all reasonable steps to prevent damage or loss to their mobile telephone. This includes not leaving it in view in unattended vehicles and storing it securely when not in use. The user may be responsible for any loss or damage if reasonable precautions are not taken.

Where a mobile telephone is lost, stolen or mislaid the following actions are to be taken:

- Inform the ICT Department of the loss and what actions have been taken (Delay in reporting could incur high costs to the Trust should the telephone fall into organised crime).
- Report the incident using the Incident Reporting

Loss through inappropriate use or lapse of security may incur costs to the user in respect of replacement charges.

Users must ensure that all mobile telephone security devices, if fitted, are enabled. This may be in the form of PIN (personal identification number) which must be an 8-digit code to meet Information Security compliance.

Staff should be aware that calls to mobile telephones are expensive (including the use of text messaging) and therefore, discussions should be CLEAR, SUCCINCT and to the POINT. Where possible, call should be made to landline numbers in the first instance. However, all Lincolnshire NHS mobile phones are on a tariff whereby all calls and texts between all Lincolnshire NHS phones are free of charge so this is preferable to calling colleagues on land lines.

The user is to understand that communications over the radio spectrum are not secure and restrict information accordingly.

All mobile phones are purchased with an international bar in place. To have the barring removed; authorisation from ICT Services must be passed to the service provider giving dates for the duration the bar is to be lifted.

Trust mobile telephones should be switched on when the member of staff is on duty or on call. There is no expectation that staff have to remain contactable at any other time.

Staff are advised under normal circumstances not to give their mobile telephone number to patients or carers. Any patient or carer who may require advice or assistance should channel their request through the existing land line telephone systems e.g. health clinic or GP surgery.

Some staff, due to the nature of their work may be required to give patients their mobile telephone number.

Staff should keep their telephone on at all times when on duty but may place in ‘silent mode’ when in contact with patients and in meetings.

Most NHS properties permit the use of mobile telephones. Use is prohibited in certain specialist hospital areas. Staff must obey relevant signs.

All requests for repair are to be directed to the ICT Department.
All upgrade requests are to be authorised by the Director / Head of Service and forwarded to the ICT Department for ordering direct with the service provider.

Upon leaving the Trust all mobile telephone equipment including SIM card and charger much be returned to the ICT Department. If a replacement member of staff is recruited to start within two weeks and is to be allocated a mobile telephone the Manager is responsible for re-issuing the mobile telephone and completing the associated paperwork.

It is an offence to use a hand held phone when driving, however provided that a phone can be operated without holding it, then hands-free equipment is not prohibited by legislation. Therefore, the use of a phone as a Sat Nav is lawful providing you don't have to hold it.

Breaches of Policy
All employees are reminded that breaches of this policy may be subject to disciplinary procedures.

CORPORATE ELECTRONIC DATA (CED)

CED is defined as:

a. All data, or information files, **created** on Trust computer software applications or computer systems. This includes data files created with any software product, such as Microsoft Outlook and Word, or any other PC/laptop based application program AND all networked systems, such as patient information or financial systems.
b. All data, or information files, **stored** on any Trust computer hardware or networked system or storage media, which includes PC or laptop hard drives and personal or shared network file storage areas.
a) All data, or information files, **electronically communicated** through Trust computer network systems. This includes both the internal and external transmission and reception of e-mail together with any attachments.

The word "owner" in relation to an electronic file is used extensively in information technology and is defined as either the file creator of an exclusively "owned" or stored file or the last person, in a group of "owners", to access a data file stored in a shared network file directory.

Despite the implications of file "ownership", staff members are advised that all Corporate Electronic Data (CED) they produce during the course of their employment remains the sole property of the employing organisation.

Sharing Corporate Electronic Data (CED)
Computer Networks offer the facility for the sharing of CED, which is commonplace, desirable and essential to business activity. However, the method and degree of CED sharing is governed by the need to know principle, organisational policies and compliance with statutory obligations such as the Data Protection Act 204 (DPA). Therefore, certain CED will demand varying degrees of higher protection by restrictive or exclusive access.

The ICT Department will create and control access to all networked CED, according to specified business need. This process is already regulated and accountable under the Computer Use codes of conduct and contracts of employment.

Responsibility
It is every member of staff's responsibility to ensure that CED that needs to be shared is made available at the appropriate time and to the appropriate individual or staff group.

Line managers are responsible for ensuring their staff makes suitable arrangements, where appropriate, to make CED available to either specific individuals or staff groups prior to embarking on training courses or annual leave with the intention of maintaining business continuity during their absence.

Business Continuity
By exception, and only to facilitate essential business continuity, there may be a requirement for senior management to access CED, which has been stored exclusively in staff's personal data areas or hard drives and become unavailable due to their absence through unforeseen circumstances.

Whilst technology exists to enable duly authorised ICT staff to access and/or make available most CED files, performing such a task on a staff member's personal computer or network data storage area, without their express permission or knowledge, should not be undertaken lightly. Strict guidelines must be followed that comply with The Regulation of Investigatory Powers Act 2000

(RIPA), and the rights and freedoms of individuals' under the Human Rights Act 1998 and other legislation.

Therefore, in the event that the maintenance of essential business continuity necessitates ICT staff to access, or give access to, otherwise unavailable CED files stored on an individual's personal user account or hard drive; **only** the Chief Executive or an Executive Director may authorise such an action.

Non-availability or corrupt data
Whilst the ICT Department will endeavour to comply with the request, it must be recognised and accepted that non-availability, corruption, password protection or encryption of the requested CED may make it impossible to comply.

ICT skills and/or the purchase of specialist hardware or software, with the inherent time delay, may enable the required access but it must be stressed that dependency should not be placed on the ICT department for a satisfactory outcome on every occasion.

Procedure
Without exception the following procedure must be adhered to:

The requesting officer, (who must be at least a line manager), should:

a. Complete a "Request & Authorisation for CED Form in full by:
    i Stating the location of the file/s – Network Drive/Folder or Laptop
    ii Identify the file/s with full path and filename, if known
    iii Where filenames cannot be given, provide a known unique and identifiable portion of text from the required file.
    iv Give the ICT Department any other assistance as may be required in finding the relevant data file/s.
    v Where access is required to an entire folder or sub-folder, state in days, the duration of such an access request.
b. Give full justification for the request.
c. Obtain appropriate authorisation from the Chief Executive or an Executive Director.
d. Ensure the request form is delivered to Senior Management in ICT.

The authorising officer should:

a. Be completely satisfied that the request is genuine and purposeful to maintain essential business continuity.
b. Be prepared to account for their personal actions, if subsequently required to by the respective organisations Board, other legal body or court of law.
c. Ensure the data owner/s is/are advised of the actions undertaken and the justification at the first opportunity.
d. Be prepared to deal with all possible and coincidental ramifications of such actions.

The accepting ICT Manager or deputy should:

a. Only initiate any action on receipt of a correctly completed and authorised form.
b. Ensure expedition of the request as soon as possible with all actions and any difficulties, including non-availability or corruption of data being recorded on the request form's action log.
c. Accessed data files are not to be amended or modified in any way. Where access is granted to data files requiring modification, copies of the original files will be placed on the storage media, specified by the requesting officer, PRIOR to any modification being undertaken. Only relocated copies of original files may be modified.
d. Strictly enforce a policy of non-disclosure or alteration of any user Passwords.

e. If a password is discovered and used to enable a positive outcome, the action should be guardedly recorded on the action log and specifically reported to the ICT Manager who must then personally advise the data "owner" at the earliest opportunity.
f. On completion, photo copy the form, file the original and ensure a copy is sent to the authorising officer for retention.

Request & Authorisation for Business Continuity
Access to Personally Stored Corporate Electronic Data (CED)

The CED contains the definitions and mandatory procedures for this process. As this request is for access to CED stored in a member of staff's personal network data storage area, PC/laptop hard drive or storage media, the requesting officer must be as specific as possible.

Accessed data files are not to be amended or modified in any way. Where access is granted to data files requiring modification, copies of the original files will be placed on the storage media, specified by the requesting officer, PRIOR to any modification being undertaken. Only relocated copies of original files may be modified.

Request

To: **The ICT Manager**, ICT Department _____ (Site Location) _____

Please enable access for: (Staff member for whom access is to be granted)

To CED "owned" by

_____

(Staff member whose files are to be accessed)

For the purpose of **(Justification Criteria)**

_____

_____

The required data is stored on: (Tick the appropriate box)

The Network ☐ The "owners" PC ☐ The "owners" laptop ☐ Storage Media ☐

Specify the data required: (Word document or Excel Spreadsheet plus file Name; etc.

_____

The file/s can be found at: (If known) _____

A filename cannot be provided but the required file contains the following unique text

_____

The located file/s should be copied to: A secure network folder (e.g. J: secure or encrypted external media:

_____

(Full path to be given – This should NOT be a shared area and should afford equivalent security to the "owners" storage area – if in any doubt, advice or assistance should be sought from Senior ICT allocated this request).

Directory Access

Where business continuity necessitates access to an entire directory or sub-directory, specify:

Directory or sub-directory name

Duration _____ (Hours / Days)

_____ (Hours / Days)

(This will be monitored and the facility revoked after the specified duration)

Requesting Officer (Line Manager (minimum)

I have read and acknowledge my responsibilities under the Business Continuity Access to Personally Stored Corporate Electronic Data (CED).

Signature _____ Date _____

Name _____ Job Title _____

Authorisation

I have read and acknowledge my responsibilities under the Business Continuity Access to Personally Stored Corporate Electronic Data (CED) Policy.

I am satisfied that this action is required to maintain essential business continuity, is appropriately justified and is therefore duly authorised.

Signature_____ Date _____

Name _____ Job Title _____

Acknowledgement by the ICT Manager or Deputy

This request form was processed by:

Name _____ Job Title _____

Signature _____ Date and Time _____

Senior ICT Action Log

(All actions and difficulties, including non-availability or corrupt data, must be recorded in narrative form clearly stating the time of action and any subsequent consequences. The log must include the specifically requested filename/s, the full paths of both where files were found and where they were copied. Where access is given to an entire directory or sub-directory, the path, access and revoke times must also be included.)

_____

_____

_____

Conclusion

I am satisfied that all possible actions have been completed, as recorded above and accordingly advised the requesting officer on date and time _____

Signature _____ Date and Time _____

ICT Manager

I advised the data “owner” (if applicable) of the reported password breach

(Date and Time) _____

Signature:_____ Date: _____

A photocopy of this completed form to be sent to the authorising office and the requesting officer for retention and the original retained by the ICT Manager for audit purposes.

MOBILE AND HOME WORKING

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 Trust.

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. The Trust is required to ensure that information security for mobile computing and home working facilities are robust enough to ensure work is conducted in a secure manner.

Mobile computing presents a very real risk to the security and integrity of Trust's information. Moreover the legislation which surrounds the way in which the Trust uses and is responsible for information makes it potentially liable for any breach or failing in security. From patient information held on laptops, to the contact details on a mobile phone to the financial spreadsheet e-mailed to a home PC, the inherent risks to information should be apparent to all staff. By recognising that the risks exist, and by implementing the controls set out, The Trust and its staff will aim to play their part in controlling them at a manageable level.

Purpose
The purpose is to provide direction for staff when working from remote locations or using mobile computer equipment throughout the Trust, to ensure compliance with acceptable standards.

Aims
The aims are:

- To ensure that the Trust 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 Trust.
- 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 Trust's reputation from being damaged by the inappropriate or improper use of its information resources.

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

Within the work environment a considerable effort in terms of money, technical knowledge and working time is expended to ensure that we maintain an appropriate level of security around the information which belongs to the Trust. Much of this information is sensitive, some of it containing clinical data and other personal details.

Personal data shall be: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'

As the use of mobile computing resources grows it is vital that the data held on these devices is not compromised by poor security practises. Mobile devices are by their very nature vulnerable to being both mislaid as well as being attractive to a potential criminal. It is important therefore that all users of mobile equipment are aware of the inherent risks associated with their use. It is now mandatory that all mobile equipment capable of storing or transporting Trust data is encrypted to the Trust's required security standards before use. If you are unsure whether or not your equipment has the necessary security applied to it please contact the ICT Service Desk for advice and assurance.

Digital Cameras used for Clinical Photography cannot be encrypted and a Risk Assessment regarding their use has been undertaken. The risk has been accepted until we can provide a satisfactorily encryption solution to digital images in transit.

This is in place to ensure information is kept securely when working from remote locations or from home and utilising mobile computing technology. Home working and working offsite must be authorised and controlled by management and suitable arrangements must be in place for this way of working to be secure. The term *"offsite working"* includes any remote working e.g. at home, on a train, in a hotel, or non-NHS premise.

All staff using mobile computing equipment or working offsite are required to comply with this policy. Failure to do so may result in this facility being removed or disciplinary action being taken against individuals'.

Duties

TITLE	INDIVIDUAL RESPONSIBILITIES
Chief Executive	As accountable Officer, has overall responsibility for the management of the Trust and for ensuring appropriate mechanisms are in place to support service delivery and continuity.
SIRO	Ensure the Trust has robust policies and procedures in place to ensure security of information held at all times.
Information Governance	Ensures the Trust has solutions in place for information security and responsibility for writing policy/procedures.
ICT Services	Ensure that technical staff provide solutions for information security in respect of mobile devices, removable media, encryption etc. To ensure that all mobile computing devices are configured in accordance with the Trust baseline measures and if used for processing patient information, that the device complies with the requirements.
Service/Line Managers	Managers are to ensure that personnel allocated mobile ICT 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. Managers must ensure that all equipment allocated for mobile working is encrypted to the Trust's 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	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. Staff must ensure that the mobile equipment they use is encrypted to the Trust's 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 ICT Service Desk.

Mobile Computing

General:

It is important to take all reasonable steps to ensure that any mobile computer device is not misplaced or stolen. This should include leaving it out of sight when away from the workplace, particularly when travelling in a car when it should be locked in the boot. In busy areas such as bus stops, railway stations or if travelling on the London Underground, it should not be placed on the ground, beside you on a counter, or left unattended at any time.

Staff must ensure that the mobile computer device is secured in a safe or other locked facility at all times when the system is left unattended especially in vulnerable locations such as an hotel or conference (if practicable).

As home environments can also be vulnerable to theft, staff are required to take appropriate precautions to reduce any risks. Mobile working devices should, where possible, be located so that they are not visible through windows from outside the home. Laptops/Notebook and PDA's in particular must be placed in a secure location when not in use.

Mobile Equipment Security:

Only Trust owned or managed equipment may be used to conduct the Trust's business or can be connected to the Trust's network. This includes all mobile working devices including:

- Laptop or Notebook computers and tablet devices
- Personal Digital Assistants – (PDA's)
- Smartphone's and other mobile phones
- External hard disk drives, USB memory sticks/flash drives
- Audio recording, photographic and video equipment - all cameras and dictation machines etc.

All mobile working equipment capable of storing and transporting any Trust data, as listed above, MUST be encrypted to the Trust's standard and asset tagged by ICT Services prior to use.

All mobile Laptop/Notebook computers must be Trust owned and purchased through the ICT Department who will then configure the equipment in accordance with the Trust base-line security measures before being used.

Smartphone's and Mobile phones must NOT be connected to the Trust's network unless they have been specifically configured and approved for this purpose by ICT Services.

Personal or privately owned electronic data processing or storage devices, which include non-NHS PC systems, flash drives, external hard disks, Smartphone's/mobile phones, photographic or audio equipment **MUST NOT** be used to conduct any Trust business or store/transport any Trust data.

External Network Connections:

Remote access to internal systems will only be authorised for Trust owned or managed equipment.

Remote access to the Trust network must be via the Trust's current authentication standard such as the Remote Access Server/VPN which provides strong authentication. These services are controlled by ICT Services. VPNs should not be carried in the same bag as the device to which they provide access. Any losses should be reported via the Trust Incident Reporting System.

Confidential data must not be e-mailed to / from a home email account or personal e-mail account. Staff must ensure that they do not download any attachments to their home pc. They must also ensure that Trust information, whether Corporate or Clinical cannot be accessed or viewed by members of their family/visitors.

Staff that have a need to use a mobile computing device to work on Trust information offsite and have been given line manager authority, are required to comply with the following:

- The equipment must be encrypted.
- The device should be afforded all reasonable protection at all times and especially whilst mobile and located away from Trust premises.
- Mobile devices must not be left unattended where it can be seen and open to theft
- The authorised user will be held responsible for the correct operation of the device and for all data processing, back-ups and storage.

Data Security Measures
Security measures are taken, within the workplace, to protect the Trust's information and many of these are legal requirements, such as the Data Protection Act. It is unacceptable for staff who wish to carry on working on Trust information within the home to simply e-mail, or remove on disk/flash drive, Trust documents to their personal equipment.

Staff are **not** to use any equipment not owned by the NHS to work on information involving patient data or corporately sensitive business information.

The use of strong password security is mandatory for all mobile computing and phone devices should use an 8 Digit Pin. In conjunction with this security feature the system should be configured to power off after a pre-determined period.

A vital aspect of mobile computing is back-ups and synchronisation. The user must ensure that adequate and regular back up measures are in place and implemented.

Staff must ensure that anti-virus software, supplied and installed by the ICT Services, is used on all mobile computing and Smartphone devices. It must be updated regularly by connecting to the Trust network where it will automatically update on connection. This software must **never** be de-activated.

Data Storage:

- All sensitive data is to be stored/and or synchronised to a Trust network or other approved secure storage system to ensure that it is backed up daily or when mobile working permits.
- Trust sensitive or confidential information is **not** to be stored on to or copied to any removable storage device unless this is appropriately encrypted to the correct security requirements. (e.g. encrypted data stick/flash drive). In certain circumstances it may be necessary to seek the permission of the relevant Information Asset Owner (IAO) to hold such data in this format and if in doubt please seek their advice/approval.
- In circumstances where there is a clear business case and the IAO consent has been given, such data may be stored on the mobile computer equipment or removable storage device providing they meet the criteria of this policy.
- All data which has been approved for storage on the mobile device is to be copied to an appropriate network drive, e.g. J Secure or other approved secure storage device, as soon as practicable to ensure that data is backed up.

Home Working

Home-working is where an employee meets their contractual obligation by working from home on an occasional or temporary basis. This includes the use of stand-alone computers and/or non-computerised working such as writing or reading reports.

The growth of information technology in recent years has increased the range of tasks, or part tasks that might be carried out by staff working from home rather than in the Trust's premises.

It is not intended that home working should be a full time arrangement except in very rare cases and special circumstances. It is intended to allow staff to have the flexibility to work part of the working week or working day at home in order to reduce commuting time and to work more flexibly around the needs of their families.

Benefits of home working
Home working may be considered as a long term arrangement or to cover a short term difficulty. It may also be considered if someone is unable to get to work e.g. because of accident or injury – or as part of a return to work strategy. It may also be considered where it may be of benefit to the service and also potentially save travel time and costs.

It should not be used where medical opinion is that the person is unfit to work.

The benefits of home working include:-

- For the Individual – greater flexibility for combining work and domestic arrangements, greater job satisfaction and personal responsibility, dedicated uninterrupted time allocated for specific project work away from the work environment.
- For the Trust – potential for increased quality and quantity of work, retention of trained staff that might otherwise leave for domestic reasons, support for equal opportunities and flexible working policies and modernisation initiatives.

Management Responsibilities
An employee requesting to work at home should be asked to complete a flexible working request. The manager will consider whether a job may be suitably adapted to a home working arrangement. In the case where this is thought to be acceptable the specific details surrounding the arrangement will be written, recorded, agreed and signed by both parties and be treated as an addendum to the existing contract of employment.

It is essential that managers have specific communication arrangements which are robust – the principle being that it should be possible to contact the employee working at home at any time during working hours, and that the employee will have access to support and advice at all times.

Risk Assessment
Managers should give full consideration to the Health and Safety aspects of employees working from their own homes and ensure that a Risk Assessment is completed and submitted by the employee concerned. It may be necessary for the Risk Assessment Manager to be involved should any areas of concern be highlighted.

Monitoring and Review
Home working arrangements should be monitored and reviewed regularly in line with the appraisal system and either amended or extended in line with Trust policy. Managers should be particularly careful to ensure people working regularly at home do not become isolated from the Trust.

Home-working/Tele-working arrangements will be carried out by mutual agreement and will not affect the employee's employment status.

Tax Relief
Tax allowance can be claimed if you work from home for 1 or more days per week, however under current HMRC rules this will only apply if it is necessary that the employee works from home, not if they merely choose to work from home.

Health and Safety Considerations
Staff must work within the guidance as set out in the Display Screen Equipment Procedure, ensuring the relevant risk assessments have been completed including any remedial actions

Staff using mobile computing equipment must take precautions to ensure that they are working in a safe and secure manner. Mobile equipment must always be physically secured when unattended.

Staff should ensure that they are applying good moving and handling techniques when carrying portable equipment. Ensure manual handing training has been undertaken in accordance with Trust policy.

Confidentiality
Staff must be aware that they have a legal duty to maintain the confidentiality of data/information taken out of the Trust for working offsite or at home, whether it is paper based or as computer files.

When confidential data has been authorised, by your line manager, to be processed offsite, users are subject to Trust confidentiality agreements and must ensure they meet the requirements of this GDPR, the Information Security Policy and the Data Protection Policy.

Staff are to Log out if they move away from the mobile device at any time, it should never be left unattended and accessible.

Lincolnshire Community Health Services NHS Trust

Allocation of Mobile Phone / Smartphone / Data Card / MiFi

PLEASE NOTE: - THIS FORM MUST ALSO BE USED FOR THE ACTIVATION OF DATA CARDS EMBEDDED IN LAPTOPS

Please note that incomplete forms may be returned for all accurate information to be completed

To be completed by Director / Head of Service

Please order and allocate a * Mobile Phone/ Smart Phone / Data Card / MiFi (also complete a remote access form for VPN access and forward to Fen House) for:-
*** Delete as appropriate***

Name (block capitals): _____

Job Title: _____

Work Base: _____

Reason for allocation: _____
(Please refer to Authorisation in the policy)

_____

_____

Does this member of staff currently have a Trust Mobile Phone / Data Card, working or not?
YES / NO (delete as appropriate)

If Yes, please indicate current Mobile Phone / Data Card number: _____

I authorise this phone for Personal Use: YES / NO (delete as appropriate)

PLEASE INDICATE MODEL NUMBER OF LAPTOP (Data Card requests only):
……..

Cost Centre: _____ Expense Code: 46405

Name (block capitals): _____

Signed: _____
(Director / Head of Service)

Date: _____

Please return completed form to: ICT Department, Arden & GEM CSU, Fen House, Fen Lane, North Hykeham, Lincoln. LN6 8UZ – or fax to 01522 563074, for the phone to be ordered and issued to the user along with a copy of the policy.

Lincolnshire Community Health Services NHS Trust

Withdrawal / Re-allocation of Mobile Phone / Smartphone / Data Card / MiFI

To be completed by Director / Head of Service

Please withdraw Mobile Phone / Data Card number / MiFi: _____

From: _____

Reason for withdrawal:

_____

_____

This Phone / Data Card / MiFi can be re-allocated to:

Name (block capitals): _____

Job title:

Work base: _____

Does this member of staff currently have a Trust Mobile Phone / Data Card / MiFi working or not?

_____

Reason for allocation: _____
(Please refer to policy)

_____

_____

I authorise this phone for personal use. YES / NO (delete as appropriate)

Financial Cost Codes: _____Cost Centre: _____Expense Code: 46405

Signed: _____
(Director / Head of Service)

Date: _____

Please return completed form to: ICT Department, Arden & GEM CSU, Fen House, Fen Lane, North Hykeham, Lincoln LN6 8UZ, who will arrange for re-allocation of the Telephone / Data Card and issue of policy.

Lincolnshire Community Health Services NHS Trust

Issue of Mobile Phone / Smartphone to individual users

MOBILE TELEPHONE NUMBER: _____

USER: _____

I declare that I have received the above mobile phone. I have also received, read and understood the associated policy with regard to its use.

Signed: _____ Date: _____

Designation: _____
(User)

I DO INTEND using the above Mobile Telephone which is in my possession for making private calls

After having read the Trust Mobile Phone and Access Policy, I agree to have £ _____ deducted from my salary on a monthly basis.

Signed: _____ Date: _____

Designation: _____
(User)

Please return this form to: ICT Department, Arden & GEM CSU, Fen House, Fen Lane, North Hykeham, Lincoln. LN6 8UZ, who will forward on to Payroll.

NHSLA Monitoring

Minimum requirement to be monitored	Process for monitoring e.g. audit	Responsible individuals/ group/ committee	Frequency of monitoring /audit	Responsible individuals/ group/ committee (multidisciplinary) for review of results	Responsible individuals/ group/ committee for development of action plan	Responsible individuals/ group/ committee for monitoring of action plan
DSPT Standards	Review / Audit / Reports	IG Lead	Annual	IG Lead / IGMAG	IG Lead / IGMAG	IG Lead / IGMAG

Equality Analysis

A.	Briefly give an outline of the key objectives of the policy; what it's intended outcome is and who the intended beneficiaries are expected to be	To provide clear and effective management and accountability structures, governance processes, documented policies and procedures, a comprehensive IG training programme and adequate resources to manage and embed IG throughout the Trust.		
B.	Does the policy have an impact on patients, carers or staff, or the wider community that we have links with? **Please give details**	All Staff and Service Users		
C.	Is there is any evidence that the policy\service relates to an area with known inequalities? **Please give details**	No		
D.	Will/Does the implementation of the policy\service result in different impacts for protected characteristics?	No		
		Yes	No	
	Disability		X	
	Sexual Orientation		X	
	Sex		X	
	Gender Reassignment		X	
	Race		X	
	Marriage/Civil Partnership		X	
	Maternity/Pregnancy		X	
	Age		X	
	Religion or Belief		X	
	Carers		X	
	If you have answered 'Yes' to any of the questions then you are required to carry out a full Equality Analysis which should be approved by the Equality and Human Rights Lead – please go to section 2			
The above named policy has been considered and does not require a full equality analysis				
Equality Analysis Carried out by:	Kaz Scott			
Date:	June 2018			