Lincolnshire Community Health Services NHS Trust

Mobile Phone and Remote Access Policy

Reference No:	P_IG_31
Version:	2
Ratified by:	LCHS Trust Board
Date ratified:	11 May 2021
Name of author:	Data Protection Officer
Name of responsible committee:	Information Governance Management Assurance Group
Date approved by responsible committee:	21 April 2021
Date issued:	May 2021
Review date:	May 2023
Target audience:	LCHS Staff
Distributed via:	LCHS 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		Full Review UK GDPR	Nov 2020 Mar 2021	Kaz Lindfield-Scott
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 • Disciplinary Policy • Flexible Working Policy (including Agile Working) • Incident Reporting Policy • Information Security Policy • Lone Worker and Violence and Aggression at Work 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 instructions and any additional advice and training will be available on issue of the devices.
Dissemination	The policy will be published on the Trust website.
Resource Implication	Cost of devices and ongoing rental to be borne by budget holders applicable to the service area.
Equality Statement	As part of our on-going commitment to promoting equality, valuing diversity and protecting human rights, Lincolnshire Community Health Services NHS Trust is committed to eliminating discrimination against any individual (individual means employees, patients, services users and carers) on the grounds of gender, gender reassignment, disability, age, race, ethnicity, sexual orientation, socio-economic status, language, religion or beliefs, marriage or civil partnerships, pregnancy and maternity, appearance, nationality or culture

MOBILE PHONE AND REMOTE ACCESS
The objectives are:

- To outline the key elements of the Trust's mobile 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
"Smartphone' is defined as a telephone not physically connected to a landline. Cordless telephones are an extension of a telephone physically connected to a landline and 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.

General Statement
Smartphones will be provided by the Trust for work related purposes at the discretion of their Line Manager.

With prior approval by the Line Manager, smartphones may be used for private purposes which will be charged to individuals in line with Inland Revenue requirements.

The smartphone is at all times the property of the Trust. Where appropriate, smartphones can be used on a pool basis but not authorised for private use.

Microsoft Teams is available to staff to allow telephone calls to me made over the internet.

Management Responsibilities
Line Managers/Budget Holder:

- Responsible for the authorisation of the purchase of smartphones.
- To notify the ICT Department of any transfers or when a member of staff leaves the Trust.
- To return equipment to ICT for cleansing and re-issue as part of Trust process

ICT Services:

- Responsible for procurement, issue and disposal of Trust smartphones where damaged or end of life.
- Will ensure all current security and safety guidelines referring to the operation of smartphones and any procedures are amended to reflect national changes.

Authorisation
The purchase of smartphones is only to be authorised for:

- Staff who work in isolation, on-call or on standby those and who need to be easily contactable during their normal working day in line with the Trust's Lone Worker and Violence and Aggression at Work Policy.
- All requests should be raised as a Service Request through the Self-Service Portal

Procurement Strategy
ICT Services

- Will process all smartphone orders upon receipt of an authorised requisition using the current contract network provider.
- Will monitor the use using the network providers monthly call statement and report any signs of misuse to the appropriate Management.

User's responsibility
The user should take all reasonable steps to prevent damage or loss to their smartphone. 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 smartphone 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 this fall into organised crime).
- Report the incident to the Line Manager and submit am IR1 through Incident Reporting.
- Any ICT Service Request /Police Incident Number should be recorded on the IR1.

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 security devices are enabled in the form of PIN (personal identification number) which must be a minimum of 8-digits to meet Information Security compliance.

Voice and IP Telephony
Software that allows staff to use a "softphone" on a laptop / PC, allowing the ability to work from anywhere. VoIP calls are directed via a telephone number, not to a fixed location. Incoming phone calls can be routed to where staff are connected to the internet to make and receive calls using the same number wherever they are located.

Trust smartphones should be switched on when on duty or on call but may place in 'silent mode' in meetings. 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 number to patients or carers but due to the nature of their work may be required to give their mobile number.

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 action through internally agreed processes.

Upon leaving the Trust all mobile telephone equipment including SIM card and charger much be returned to the ICT Department for wiping of data and reissue.

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.

Smartphones
These may be used for taking clinical images for evidence purposes. These will have a minimum 8-digit pin applied and are fully encrypted. Changing the 8-digit pin to a pattern is against Trust policy and must remain as a pin code. This is Trust issued equipment only to be used, not personally owned.

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

CORPORATE ELECTRONIC DATA (CED)
CED is defined as:

a. All data **created** on Trust computer software applications or computer systems. This includes data files created with any software product, such as Microsoft Office, or any other PC/laptop based application program AND all networked systems, such as personal information or financial systems.
b. All data **stored** on any Trust computer hardware or networked system or storage media to include OneDrive and SharePoint, C or laptop hard drives and personal or shared network file storage areas.
a) All data **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 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 are advised that all CED) they produce during the course of their employment remains the sole property of the employing organisation.

Sharing Corporate Electronic Data
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 sharing is governed by the need to know principle, organisational policies and compliance with statutory obligations such as the Data Protection Act 2018 (DPA). Therefore, certain data will demand varying degrees of higher protection by restrictive or exclusive access.

The ICT Department will create and control access to all networked data, 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 data 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 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 data, 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 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 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, Executive Director or Data Protection Officer 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 data 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 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 Provide 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, an Executive Director or Data Protection Officer.
d. Ensure the request form is delivered to Senior Management in ICT.

The authorising officer should:

a. Be completely satisfied the request is genuine and purposeful to maintain essential business continuity.
b. Be prepared to account for personal actions, if subsequently required to by the respective 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 action log.
c. Accessed data files are <u>not</u> 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 advise the data "owner" at the earliest opportunity.
f. On completion, 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)

This contains the definitions and mandatory procedures for this process. As this request is for access to data stored in a member of staff's 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. 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 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 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.

Purpose

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

Aims

The aims are:

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

The applies to all employees of the Trust, 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.

Personal data shall be processed in a manner that ensures appropriate security of the 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 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 required security standards before use.

Digital Cameras cannot be encrypted and a Risk Assessment regarding their use has been undertaken. The risk has been accepted and the Trust has now provided Smartphones which are encrypted to hold digital images in transit.

All staff using mobile computing equipment or working offsite are required to comply and 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 the security of information held at all times.
Data Protection Officer	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

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 the 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).

Home environments can also be vulnerable to theft, staff are required to take appropriate precautions to reduce any risks. Mobile devices should, where possible, be located so that they are not visible through windows from outside the home. Laptops/Smartphones 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 tablet devices
- 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 Laptop/Tablet 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.

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

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 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 through the Trust's current authentication standard such as VPN which provides strong authentication.

Personally Identifiable Information (PII) must not be e-mailed to / from a personal e-mail account e.g. Gmail, Hotmail. Staff must ensure they do not download any attachments to a home pc. They must also ensure that Trust information, whether Corporate or Clinical cannot be accessed or viewed by members of family/visitors.

Staff that 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 used is encrypted.
- The device should have protection at all times 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 responsible for the correct operation of the device and 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, to their personal equipment.

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

The use of strong password/passphrase is mandatory for all mobile computing devices which should use an 8 Digits minimum. 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.

Anti-virus software is installed by the ICT Services and 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 or when mobile working permits.

- All data which has been approved for storage on the mobile device is to be copied to an appropriate network drive, or other approved secure storage device, as soon as practicable to ensure that data is backed up.

Home Working
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 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:-

- 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.
- 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
Employees can have informal arrangements with their line managers regarding working flexibly and 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 the employee will have access to support and advice at all times.

Risk Assessment
Managers should consider the Health and Safety aspects of employees working from their home and ensure that any Risk Assessment is completed.

Monitoring and Review
Home working arrangements will be monitored and reviewed in line with Trust decisions which may affect the Health, Safety and Welfare of Staff e.g. Pandemic. Managers should be particularly careful to ensure people working at home do not become isolated from the Trust.

Home-working arrangements 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 HMRC rules this may only apply if it is necessary the employee works from home and advised to check the latest guidance.

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 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 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 electronic and must ensure they meet the requirements of this GDPR, the Information Security Policy and the Data Protection Policy.

Staff are to Log out/lock their screen if they move away from the mobile device, it should never be left unattended and accessible.

NHSR 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	DPO	Annual	DPO / IGMAG	DPO / IGMAG	DPO / IGMAG

Equality Impact Analysis Screening Form

Title of activity	Mobile Phone and Remote Access Policy		
Date form completed	Mar 2021	Name of lead for this activity	Kaz Lindfield-Scott

Analysis undertaken by:		
Name(s)	Job role	Department
Kaz Lindfield-Scott	Data Protection Officer	Data Protection and Compliance

What is the aim or objective of this activity?	To provide effective management and accountability governance structures, processes, policies and procedures and a comprehensive IG/DP training adequately resourced to manage and embed IG and DP throughout the Trust.
Who will this activity impact on? *E.g. staff, patients, carers, visitors etc.*	All Staff and Service Users

Potential impacts on different equality groups:

Equality Group	Potential for **positive** impact	**Neutral** Impact	Potential for **negative** impact	Please provide details of how you believe there is a potential positive, negative or neutral impact (and what evidence you have gathered)
Age	☐	☒	☐	
Disability	☐	☒	☐	
Gender reassignment	☐	☒	☐	
Marriage & civil partnerships	☐	☒	☐	
Pregnancy & maternity	☐	☒	☐	
Race	☐	☒	☐	
Religion or belief	☐	☒	☐	
Sex	☐	☒	☐	
Sexual Orientation	☐	☒	☐	
Additional Impacts	☐	☒	☐	

If you have ticked one of the above equality groups please complete the following:

Level of impact

	Yes	No
Could this impact be considered direct or indirect discrimination?	☐	☒
If yes, how will you address this?		

	High	Medium	Low
What level do you consider the potential negative impact would be?	☐	☐	☐

If the negative impact is high, a full equality impact analysis will be required.

Action Plan

How could you minimise or remove any negative impacts identified, even if this is rated low?
How will you monitor this impact or planned actions?
Future review date: