NHS
Pennine Care
NHS Foundation Trust

DOCUMENT CONTROL

Title:	**Mobile Device Usage & Security Policy**
Version:	**6**
Reference Number:	**HI003**

Scope:

This policy applies to all staff using mobile devices issued by Pennine Care NHS Foundation Trust.

Purpose:

This document sets out the Pennine Care NHS Foundation Trust's policy for the use and security of mobile Health Informatics devices and mobile telecommunications devices, the rules relating to use(s) and the consequences that may arise from misuse. The policy relates to mobile devices owned and managed by Pennine Care.

Keywords:

Mobile Device Usage, Phones, Laptops, iPhone, Tablets, iPads, Smartphones

Supersedes:

Version 5

Description of Amendment(s):

- Updated with new ICT Service Desk telephone number
- Document updated to include use of iPhones
- Digital dictation devices included
- Updated to include installation and charges of "apps "
- Use of personal smart phones for NHSmail
- Reasonable adjustment section added
- Harmonised following TCS (Transforming Community Services)

Owner:

Chief Information Officer – Chris Reynolds

Individual(s) & group(s) involved in the Development:

This document has been developed in collaboration with the following interested parties:

- Head of ICT – Robert Brocklehurst
- Chief Information Officer – Chris Reynolds

Individual(s) & group(s) involved in the Consultation:
The document has been circulated for consultation and comments have been taken into consideration and the document amended accordingly: • Health Informatics Steering Group

Equality Impact Analysis:	
Date approved:	30th July 2018
Reference:	HI003 – EIA003
Freedom of Information Exemption Assessment:	
Date approved:	18th July 2018
Reference:	2018/0644
Information Governance Assessment:	
Date approved:	18th July 2018
Reference:	2018/0644
Policy Panel:	
Date Presented to Panel:	23rd July 2018
Presented by:	Chris Reynolds
Date Approved by Panel:	23rd July 2018
Policy Management Team tasks:	
Date Executive Directors informed:	21st August 2018
Date uploaded to Trust's intranet:	25th July 2018
Date uploaded to Trust's internet site:	25th July 2018
Review:	
Next review date:	July 2021
Responsibility of:	Chief Information Officer

Other Trust documentation to which this guideline relates (and when appropriate should be read in conjunction with):	
CO014	Information Security Policy Manual
CO026	Personal Computer Policy.
CO051	The Policy for Electronic Transfer of Patient Identifiable data.
HI001	The Policy for the permitted use of removable media.
CO061	Network Security Policy
CO010	Trust Incident Policy
CO033	Display Screen Equipment Policy
IG002	Data Protection and Confidentiality Policy
CO044/CO020	IG and records management suite of policies
CO109	IG Staff Handbook

Policy Associated Documents:	
TAD_HI003_01	Specific Terms of Use for Smart Phone Devices
TAD_HI003_02	Specific Terms of Use for Laptops that are wireless capable
TAD_HI003_03	Workstation Self-Assessment Checklist
TAD_HI003_04	Mobile Device / Laptop Acceptance Form
TAD_HI003_05	Request to use Personal Mobile Device to Access NHS Mail.
Other external documentation/resources to which this guideline relates:	
	• Health and Safety at work Act 1974 • Provision of Work Equipment Regulations 1998
CQC Regulations **This guideline supports the following CQC regulations:**	

Contents Page

1.	Introduction	5
2.	Purpose	5
3.	Responsibilities, Accountabilities & Duties	5
4.	Mobile Devices and their uses	8
5.	Risks	9
6.	Guidance for Use	10
6.1	Security	10
6.2	Health & Safety	11
6.3	Use of Mobile Telephones	11
6.4	Use of Mobile Devices or Laptops whilst Driving	12
6.5	Protecting the Trusts Computer Network	12
6.6	Safeguarding Information	13
7.	Disciplinary Considerations	14
8.	Reasonable Adjustment	14
9.	Equality Impact Analysis	14
10.	Freedom of Information Exemption Assessment	15
11.	Information Governance Assessment	15
12.	Safeguarding	15
13.	Monitoring	15
14.	Review	15

1. INTRODUCTION

Mobile devices are important to the Trust as they can allow staff to work more effectively in places where using a desktop computer would be impractical. Mobile devices such as laptops, mobile communication devices (e.g. mobile phones or smart phones), dictation devices and digital cameras allow staff to achieve more by providing facilities on the move. Eventually, many of our staff will be using mobile devices to enable them to work more efficiently and effectively. This is why this policy and associated policies are important.

As part of the office environment, ICT equipment and associated services are provided to staff to access resources required to complete their role. Personal issue of ICT hardware is intended to provide the capability for remote and/or mobile accessibility to Trust systems for Pennine Care staff, and as such are intended to enhance operational efficiency and effectiveness. All Trust employees that are issued with mobile devices are required to have read and agree to this policy and related policies. Any breach of this policy will be treated as a potential disciplinary issue.

2. PURPOSE

This document sets out the Pennine Care NHS Foundation Trust's policy for the use and security of mobile Health Informatics devices and mobile telecommunications devices, the rules relating to use(s) and the consequences that may arise from misuse. The policy relates to mobile devices owned by Pennine Care.

A significant cost is attached to developing and deploying mobile assets and the Trust must demonstrate that its investment is optimised by ensuring that best practice in Health Informatics asset procurement, management and usage is embedded across the Trust.

This policy should be read in conjunction with the policies in stated on the control page

3. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

Responsibilities that the Pennine Care NHS Foundation Trust delegates to all its employees that are issued with mobile device(s) are listed below.

3.1 Users of mobile devices are responsible for ensuring their safe keeping. Despite their portability, mobile devices are valuable assets and must be treated as such. In the event of damage, loss or theft of the mobile device, the user must immediately notify the Pennine Care Health Informatics ICT Service Desk on 0161 716 1234, quoting the police crime reference number if appropriate.

3.2 Prior to the release of any mobile device, users must read and sign a user acceptance form which clearly outlines the user's responsibility in regard to the device. The mobile device acceptance form can be found in TAD_HI003_04.

3.3 Mobile devices are provided for use by the employees of the Trust and access is prohibited to non-Trust employees unless approved by Information Governance

3.4 Mobile devices must remain in the possession of the Trust employee that has signed for the device. Any transfer of equipment must be authorised by the Health Informatics Department in order to maintain the accuracy of the Trust's inventory.

Failure to inform the Health Informatics Department will lead to the person signing the original agreement being held responsible for the equipment.

3.5 Patient identifiable or sensitive data should not be stored on the mobile device at any time. If digital cameras are used to capture patient images e.g. medication identification, then consent should be obtained in accordance with Trust policy. The images must be uploaded onto the Trust network as soon as possible and then deleted from the camera in accordance with Trust policy. If video equipment is used, with client consent, to record client sessions, the tape (or other media) must immediately be removed from the video on completion of the session and stored securely. No more than one patient session should be recorded on the tape at any one time. Approval must be sought from the Information Governance Manager if recorded images are provided to external organisations for example sent to university for research or part of professional qualification training. Please see policy Electronic Transfer of Person Identifiable Data (CO51) for further information.

3.6 Trust employees are prohibited from installing any additional software on Trust purchased equipment, with the exception of smart phone devices. Staff can install additional “apps”* on smart phone devices but any cost associated with the software purchased will remain the liability of the individual staff member. The Trust will not be held responsible for any costs related to these purchases.

3.7 Damage caused by deliberate act of abuse or neglect of the mobile device, or employees failure to follow Trust policies will result in the employee being held responsible for the cost of repair.

3.8 Use of mobile telephone equipment for personal use is permitted by the Trust on the basis that costs incurred for personal use will be recovered from the user. Personal calls can be identified by placing an asterisk at the end of the number dialled. All costs associated with “apps” downloaded by staff will also be considered as personal use. Arrangements for recovering personal usage costs directly from the user’s salary can be made by contacting the ICT Service Desk.

3.9 Staff who wish to use their personal equipment such as their own smart phone to synchronise to their NHSmail account, must complete the request form see TAD_HI003_05 of this policy. The form should be completed and returned to the Health Informatics department for approval. Only once approval has been given are staff authorised to use their personal device. All costs associated with using personal devices to access Trust systems will remain the liability of the staff member and NOT the Trust. Each time a staff member that has been approved to use their personal mobile device changes that device, a new request form must be completed. Services which are funded by another agency, e.g. University should consult with the Trust Information Governance Manager to ensure appropriate policies are agreed with the funding organisation. Please be aware that the Trust monitors connections to the network, and anyone connecting their personal mobile smart phone without authorisation, will be contacted and asked to either complete a form, or remove the device settings.

3.10 Passwords or passcodes relating to mobile devices should never be written down or kept with the device.

Employees should fully understand what is required of them and they must adhere to the terms of use at all times. Additional specific terms of use for mobile phone and smartphones can be found in TAD_HI003_01 and specific terms of use for mobile laptops away from the office can be found inTAD_HI003_02. The following points give further background on how devices are / should be managed:

3.11 When Health Informatics is notified by ESR that a staff member is leaving the Trust, ICT will contact the line manager to confirm the location of devices known to the leaver. The line manager will be either requested to return the equipment if the leaving employee will not be replaced, or provide details of the replacement and the required Mobile Device Acceptance form (TAD_HI003_04) for the new starter. If there is a period of time between the staff member leaving and the new starter, then the line manager will be responsible for the equipment. On occasion the Health Informatics Team may request that the equipment is returned to enable a fresh re-installation of software.

3.12 All mobile devices are encrypted. In order to ensure synchronization all mobile devices must be connected to the Trust network at least every 90 days.

3.13 Unauthorised copying of software is illegal as defined by copyright law. Any data corruption or configuration errors caused by the unauthorised installation of software may result in the loss of all data on the smart phone device, for which the Trust will not be held responsible.

3.14 The Health Informatics Department will be responsible for providing support related to issues concerning the operation / use of the mobile devices provided the Trust policy has been adhered to. During fault finding Health Informatics may require the mobile device to be reset back to the original factory settings. Health Informatics are not responsible for re-installing any ‘apps’ or ‘app’ settings relating to ‘apps’ installed by the employee.

3.15 Trust mobile devices must be procured by the Health Informatics Department. Individual departments are not permitted to purchase their own devices without prior agreement of the Health Informatics department.

3.16 Trust purchased mobile devices must be returned to the Health Informatics department when requested for health check or audit.

3.17 Configuration & settings on Trust mobile devices should only be altered or removed by Health Informatics staff.

3.18 The Health Informatics department will monitor mobile device usage for excessive use and will bring any issues to the attention of the staff member and their line manager.

3.19 All mobile devices will be configured for national and local voice \ data access only. Premium \ international calls and international data roaming will be barred. International call barring and data roaming can be lifted for specific periods on approval of the relevant budget holder, however staff must be aware that use of voice or data roaming whilst abroad will result in additional cost to the current applied tariff. To request access, staff must complete the authorisation form “Request for international voice \ data roaming” which is available on the Health Informatics intranet page. Requests must be received 5 working days prior to the requested start date to ensure barring is lifted for the requested period.

4. MOBILE DEVICES AND THEIR USES

4.1 The types of mobile device currently used within the Trust are:-

Laptops – these are computers that can be transported anywhere and used without requiring mains power for the most part. Laptops allow their users to look at, create or modify information in accordance with the Trust’s Information Security Policy. Laptops can have mobile broadband built in, providing capabilities of accessing the internet and the Trust network (VPN) where usage must be in accordance with the Trust’s Personal Computer Policy and Network Security Policy. The Trust will also ensure that all laptops are fully encrypted to DOH standards (AES 256).

Mobile Phone – is a device that allows the ability to make telephone calls and send \ receive text messages without the need for a physical connection to a telephone network. They are different to a Smartphone as described below.

Smart Phone – a smart phone provides the same functionality as a mobile phone with the additional ability of being able to send \ receive emails, access the internet, take digital photographs or sound \ video recordings and enable the use of applications (apps).

Digital Cameras & Camcorders – allow the user to capture images in a digital format that can then be transferred onto the corporate network. The images/pictures should be work related and can be transferred physically via a cable connected to the Trust computer. There is no Trust standard digital camera at present.

Video recorders – Allow the user to record moving images e.g. training presentation. The recording must relate to work. The use of video recording equipment for client sessions must be with the informed consent of the client and the follow guidance provided throughout this policy must be adhered to. There is no standard Video recorder at present.

Digital Dictation units – Allow the user to record speech and store these recordings in a digital format that can then be transferred on to the corporate network. The recording must relate to work. The use of audio recording equipment for client sessions must be with the informed consent of the client and guidance provided throughout this policy must be adhered to.

4.2 Other devices may be added to this list in the future. The key features of any mobile device are that they are portable, and have the potential of holding data. Due to the portable nature of these devices they must be managed strictly in accordance with Trust policies as described in Section 3.2 of this document.

4.3 The Health Informatics Department will maintain a set of standard specifications for all of the above items which will meet user requirements for speed and functionality.

Where a non-standard specification is required to meet specific business requirements this will require the agreement of the Health Informatics Department.. The latest specification for each type of mobile device is available on the Trust's intranet or from the ICT Service Desk.

5. RISKS

5.1 Mobile devices have the potential to deliver significant benefits. However they can also carry a number of risks, including:

- Cost of loss or damage to expensive equipment as a consequence of theft, carelessness or misuse.
- Health and safety problems for users, if equipment is used incorrectly.
- Introduction of viruses to the Trust computer network if devices become infected if appropriate precautions are not taken (for example updating antivirus software)
- Disruption of the Trust computer network if incompatible devices are connected.
- Increased demand on Health Informatics services
- Loss of data contained on mobile devices and consequent disruption to work. (This has been minimised by the encryption of devices, and the introduction of the Permitted use of Removable Media Policy/Electronic Transfer of Patient Identifiable Data Policy).
- Disclosure of confidential/sensitive information accessed via devices as a consequence of loss of devices or careless use.
- Potential financial costs if mobile phone/data downloads are abused.
- Risk to the reputation of the organization as a trusted provider of health care services

5.2 The aim of this Policy is to enable the Trust to benefit from the new technologies that are available, whilst managing the above risks. The risks are unlikely to be eliminated, but can be mitigated through compliance with this and associated policies. Given that there will remain inherent risks associated with the use of mobile devices, it is important that clear business benefits can be demonstrated, wherever they are used, which outweigh those risks.

5.3 The key to managing all of the above risks is ensuring that users conform to some basic rules and good practice guidelines. For that reason all users will be asked to sign a mobile device acceptance form, (TAD_HI003_04) or complete the request to use personal mobile device form (TAD_HI003_05), acknowledging their responsibilities.

6. GUIDANCE FOR USE

6.1 Security

To avoid loss or damage to mobile devices the following guidelines should be adopted by Trust employees at all times.

6.1.1 The mobile device should always be transported in its original case or a case designed for the device and stored carefully so it is not susceptible to damage. Other items should not be loaded on top of the device, even if the device is in its storage case.

6.1.2 Mobile devices not in use must be switched off or placed in hibernate mode and where appropriate placed in the approved carrying case. The devices should prompt for a password when the device is re-started for use i.e. must be left in a locked state.

6.1.3 The mobile device should not be left inside a vehicle where temperature extremes can permanently damage the unit and/or its components. They should be stored securely in the vehicle's boot during transit. Mobile equipment should not be left unattended in a vehicle, however in circumstances where this is not possible, the device should be stored out of sight, i.e. in the boot of the vehicle.

6.1.4 The mobile device should not be left unattended in an unsecured area; i.e. clinical rooms, reception area, areas accessible by the public or non-employees of the Trust. When not in use the mobile device should be locked in a cabinet or desk and should not be left visible. The Trust will provide a Kensington lock for laptops to provide additional security, employees must ensure that the locks are used and the associated keys kept safe. In the event of an emergency, reasonable effort should be made to secure the mobile device, but **NEVER** at the expense of staff safety

6.1.5 In the event of a mobile device being lost or stolen users should immediately inform their line manager, and log this with the Health Informatics Service Desk on 0161 716 1234 . An incident form must be completed on the Trust incident reporting system. If the equipment has been stolen the police should be contacted to obtain a crime reference number. If the device contained patient information, which would be in breach of this policy, the patient should be informed after agreement with the clinical team as to who should inform the client and what clinical support should be in place for the client out of hours. If staff that have lost an approved personal device for accessing NHSmail, then they should also contact the Health Informatics Service Desk for advice on how to remotely securely wipe the device.

6.1.6 Care must be taken to avoid touching the screen of the mobile device. Fingerprints on the screen can be removed using appropriate screen wipes. (This is with the exception of touch screen devices) Abrasive solutions or cleaning material should not be used.

6.1.7 Care must be taken to avoid spillage of drinks and other liquids close to any mobile device. In the event of accidental spillage the mobile device must be switched off immediately and the Health Informatics Service Desk contacted on 0161 716 1234.

6.1.8 All Trust mobile equipment is security marked – these marking should not be tampered with or removed.

6.1.9 Password settings should **NEVER** be removed. Passwords should be in line with the Trust's password complexity standard as enforced on the specific device / application.

6.1.10 It is safe to allow airport security to x-ray mobile devices.

6.2 Health and Safety

6.2.1 Exact Health and Safety procedures will vary from device to device, but some general guidance is found in the Display Screen Equipment Policy. Staff should always refer to the Trust Health and Safety policies for detailed information. TAD_HI041_03 has a DSE assessment check list, which can be used to provide some general guidance. Some simple steps that can be taken to improve Health and safety when using mobile devices are;

- Staff should take regular breaks when using display screen equipment and ensure good posture.
- Staff should not type for longer periods than is comfortable.
- Laptop cases should not be loaded with excessive amounts of additional items such as books. Staff may need to use a wheeled device to transport portable devices to avoid back strain.
- Staff must be aware about trip hazards from trailing wires and conduct a risk assessment to identify environmental issues such as poor lighting, distractions and posture (TAD_HI041_03). This is a requirement under DSE regulations.
- Laptops should not be used on laps or armchairs at all as this is a bad posture. This is not recommended in DSE regulations.
- Mobile devices should not be operated whilst in control of a vehicle.

6.3 Use of Mobile Telephones

6.3.1 The Stewart Enquiry into mobile telephones and health consequences determined that "The balance of evidence does not suggest mobile phone technologies put the health of the general population of the UK at risk. Preliminary evidence suggests some cases of subtle biological effects but these do not mean the health is affected." However, prudence recommends that:-

- Mobile devices that are wireless enabled should be used for as short a time as possible.
- Only mobile devices with low Specific Absorption Rate (SAR) values should be used.

- Mobile phones, Smartphones and mobile device(s) that use GPRS/wireless technology should be treated in the same manner.

6.4 Use of Mobile Devices or Laptops Whilst Driving

On 1 December 2003, it became an offence to use, or cause or permit another person to use, any hand-held mobile telephone or similar mobile device whilst driving a road vehicle. 'Hand held usage' includes, picking up a mobile device to speak to, listen or access any sort of data and includes periods when stopped in stationary traffic. Staff are not permitted to use Trust issued mobile devices whilst driving.

6.4.1 Holding and operating a mobile device whilst driving may reduce concentration and effectiveness. Using hands free equipment is also likely to distract attention from the road and may contribute to the likelihood of an accident. Pennine Care NHS Foundation Trust supports responsible national legislation to promote the safe use of mobile devices whilst driving. Responsibility for the safe control of vehicles always rests with the driver and Pennine Care NHS Foundation Trust strongly advises all staff **NEVER** to use a hand held mobile device or to use hands free equipment whilst driving.

6.4.2 There are five key points that should be followed to ensure safety:

- Whilst driving staff must **NEVER** use a hand-held mobile device for voice conversation, text messaging, or any other purpose.
- Staff should only use a mobile device when it is safe to do so, when the car is stationary and the engine switched off.
- Staff are not expected to make or receive calls or texts whilst driving.
- Staff should divert calls to voice messaging whilst driving and respond when their journey ends or at an appropriate rest point, if their mobile device rings whilst they are driving, they should ignore it until they can safely park and deal with the call.
- Staff should only use a hands-free mobile device when it is safe to do so. They must judge for themselves when it is safe to make a hands free call taking into account the driving conditions that prevail. Staff are under no obligation to make or continue calls where they have concerns that it may not be safe

6.4.3 The Trust will not take responsibility or be liable in any way for legal charges or other consequences of using a mobile device whilst driving.

6.5 Protecting the Trust's Computer Network

6.5.1 Virus infections can be introduced to the Trust computer network from mobile devices that become infected and then pass this onto the network when reconnected. In this context staff must ensure that they use mobile devices in accordance with the Information Security Policy that clearly outlines responsibility in relation to data management. The use of removal media such as 'pen-drive' or ‘flash drive’ should be in accordance with the policy for the permitted use of removable media. The following rules are designed to minimise the chances of a mobile device/laptop causing damage or disruption to the Trust’s computer network. Further guidance for mobile/wireless laptops can be found in TAD_HI003_02, which must be read in context of this subject matter.

6.5.2 Virus checking software must not be disabled, or settings altered by any Trust employee other than those working within the technical section of the Pennine Care Health Informatics Department.

6.5.3 All software installation for mobile devices must be carried out by authorised Pennine Care Health Informatics staff only. With the exception of installing personal procured “apps” on smart phone devices.

6.5.4 In circumstances where a third party is to install software, specific authority must be sought from the chief Information Officer / Head of ICT Service Delivery.

6.5.5 Unauthorised mobile devices (personal equipment or mobile devices owned by third parties) must not be connected to the Trust’s network. If staff believe that a mobile device would improve their working practices this must be discussed with their line manager, under no circumstances should they use their own personal equipment to store any Trust information or data.

6.5.6 Storage of excessive personal, identifiable data is breach of the General Data Protection Regulation (2016), and takes up unnecessary space on the network.

6.5.7 Mobile devices connected to the Trust network should not be connected to any other networks via wireless, mobile broadband, infra-red, Bluetooth at the same time in line with the NHS Digital Code of Connection.

6.6 Safeguarding Information

6.6.1 Information Security is a primary concern for the Trust. Information flow from the Trust to the outside world must be properly controlled with sensitive (or personal) information never being allowed out to third parties without express authorisation and without appropriate levels of encryption. Electronic data transfer should only be completed in strict accordance of the policy for Electronic Transfer of Personal Identifiable Data; this policy also includes Trust sensitive data that may not include personal identifiable data. Key guidance on security of information is:-

- Staff must ensure that use of hardware, software and data complies with the requirements of the relevant Data Protection legislation. The Information Governance Manager should be contacted for further details.
- All files and information on mobile devices should be backed up regularly to network servers.
- Staff must be aware of the need to protect confidential documents when working in a public place and ensure that these are not visible to others. Device screens must be locked when the user is away from them.

- The use of external storage devices to transport personal or sensitive data, whether it is directly connected to the PC or wirelessly, is prohibited. The Trust has established a process for approving the transportation of specific data types on a case by case basis; this process is detailed within Electronic transfer of Person Identifiable Data Policy
- If the mobile device has wireless capability this must be password protected and must be disabled when not in use.
- All laptops will have the Trust's encryption software installed. If staff experience any problems, or if it is found that the software is not working correctly the Health Informatics Department must be informed immediately. The laptop should not be used until advised by a member of the technical team within Pennine Care Heath Informatics Department.
- Staff must only use their personal mobile devices once formal approval has been given by the Health Informatics Department, and not on the submission of the request to use personal mobile device form.

7 DISCIPLINARY CONSIDERATION

The Trust views data security very seriously. Any breach of this policy will be investigated; each case will be considered on its own merit and could lead to disciplinary measures being taken.

8. REASONABLE ADJUSTMENT

Reasonable adjustments will be made where possible to address potential issues in terms of disability and usage of equipment. The process for reasonable adjustments is outlined in the Trust Recruiting and Retaining Disabled Staff Policy. Guidance can also be sought from the Equality and Diversity Team, HR and Health and Safety departments in relation to specific issues.

9. EQUALITY IMPACT ANALYSIS

As part of its development, this document was analysed to consider / challenge and address any detrimental impact the policy may have on individuals and or groups protected by the Equality Act 2010. This analysis has been undertaken and recorded using the Trust's analysis tool, and appropriate measures will be taken to remove barriers and advance equality of opportunity in the delivery of this policy / procedure

10. FREEDOM OF INFORMATION EXEMPTION ASSESSMENT

Under the Freedom of Information Act (2000) we are obliged to publish our policies on the Trust's website, unless an exemption from disclosure applies. As part of its development, this policy was assessed to establish if it was suitable for publication under this legislation. The assessment aims to establish if disclosure of the policy could cause prejudice or harm to the Trust, or its staff, patients, or partners. This assessment has been undertaken using the Trust's Freedom of Information Exemption Guide, and will be reviewed upon each policy review.

11. INFORMATION GOVERNANCE ASSESSMENT

This Policy has been analysed to ensure it is compliant with relevant information law and standards as in place at the time of approval, and are consistent with the Trust's interpretation and implementation of information governance components such as data protection, confidentiality, consent, information risk, and records management.

Compliance will be reviewed against any changes to legislation / standards or at the next review of this document.

12. SAFEGUARDING

All staff have a responsibility to promote the welfare of any child, young person or vulnerable adult they come into contact with and in cases where there are safeguarding concerns, to act upon them and protect the individual from harm.

All staff should refer any safeguarding issues to their manager and escalate accordingly in line with the Trust Safeguarding Families Policy and Local Safeguarding Children/Adult Board processes.

13. MONITORING

The effective application of this policy / guideline, including adherence to any standards identified within will be subject to monitoring using an appropriate methodology and design, such as clinical audit.

Monitoring will take place on a biannual basis and will be reportable to the Quality Group via the Clinical Effectiveness and Quality Improvement Team.

14. REVIEW

This policy / guideline will be reviewed three-yearly unless there is a need to do so prior to this; e.g. change in national guidance.