NHS
Pennine Care
NHS Foundation Trust

DOCUMENT CONTROL

Title:	**Electronic Mail Policy**
Version:	**8**
Reference Number:	**HI002**

Scope:

This policy applies to all users accessing the NHS mail service, via the Trust network. This policy applies to all information sent or received via the NHS mail Service via the Trust Network.

Purpose:

The objective of this policy is to explain to users of the NHS mail service, accessed via the Trust network, how the service should be used.

The purpose is to ensure the proper use of the Trust's email system and make users aware of what the Trust deems as acceptable and unacceptable use of its email system.

Keywords:

Email, NHS Mail, Outlook, Signature, Out of Office

Supersedes:

Version 7 – This policy was previous a Corporate policy CO06 – Agreed to move all IT policies under Health Informatics (HI)

Description of Amendment(s):

- Updated to include Data Protection Laws and changes to Encryption Guidance

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:

- Health Informatics Management Team

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 – April 18

Equality Impact Analysis:	
Date approved:	22nd of May 2018
Reference:	HI_EIA002
Freedom of Information Exemption Assessment:	
Date approved:	24th of May 2018
Reference:	2018/0642
Information Governance Assessment:	
Date approved:	2nd of May 2018
Reference:	
Finance Strategy Committee:	
Policy Panel:	
Date Presented to Panel:	3rd of May 2018
Presented by:	Chris Reynolds
Date Approved by Panel:	3rd of May 2018
Policy Management Team tasks:	
Date Executive Directors informed:	22nd of May 2018
Date uploaded to Trust's intranet:	24th of May 2018
Date uploaded to Trust's internet site:	24th of May 2018
Review:	
Next review date:	May 2021
Responsibility of:	Chief Information Officer
Other Trust documentation to which this guideline relates (and when appropriate should be read in conjunction with):	
CO4	Confidentiality Policy
CO13	Information Sharing Policy
CO20	Records Management Policy
Other external documentation/resources to which this guideline relates:	
CQC Regulations **This guideline supports the following CQC regulations:**	

Contents Page

1. INTRODUCTION

This document defines the Email policy for Pennine Care NHS Foundation Trust and:

- Sets out the Trust policy for the protection of the confidentiality, integrity and availability of the email system.
- Establishes organisational and user responsibilities for the email system.
- Provides reference to guidance relevant to this policy.

The NHS mail service has been provided to aid the provision of health and social care and this should be the main use of the service.

The Trust utilises the NHSmail service provided through the Health and Social Care Information Centre (Known as NHS Digital)

Compliance with Trust policies is a condition of employment and breach of a policy may result in removal of access to an email account and/or disciplinary action.

2. PURPOSE

The objective of this policy is to explain to users of the NHS mail service, accessed via the Trust network, how the service should be used.

The purpose is to ensure the proper use of the Trust's email system and make users aware of what the Trust deems as acceptable and unacceptable use of its email system.

3. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

Legal Risks

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature, email seems to be less formal than other written communication, the same laws apply. Misuse of email may contravene one or more of the following:

- Current Data Protection laws
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Law of Copyright
- The Electronic Communications Act 2000

Therefore, it is important that users are aware of the legal risks of email.

If you send or forward emails with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions, you and the Trust can be held liable.

If you unlawfully forward confidential information, you and the Trust can be held liable.

If you send an attachment that contains a virus, you and the Trust can be held liable.

All Users Must Not:

- Use the NHSmail service to violate any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is usually grounds for dismissal and any illegal activity will be reported to the police. Illegal activity includes, but is not limited to, sending or receiving material related to paedophilia, terrorism, incitement to racial harassment, stalking and sexual harassment and treason. Use of the service for illegal activity will result in the immediate suspension of the user's NHSmail account.

- Use NHSmail accounts for regular personal use. A personal email account should be set up with an internet provider (see Section 19 for further guidance on personal use).

  - All communication you send through the NHSmail service is assumed to be official correspondence from you acting in your official capacity on behalf of the organisation. Should you need to, by exception, send a communication of a personal nature you must clearly state in the subject field that your message is a personal message and not sent in your official capacity and remove any details from your email signature i.e. job title, work location and contact details.

  - Use the NHSmail service for commercial gain or to run a business.

  - Use the NHSmail service to disable or overload any computer system or network.

  - Use the NHSmail service to harass other users or groups.

  - Attempt to interfere with technical components, both hardware and software, of the NHSmail system in any way.

  - Attempt to disguise your identity or your sending address.

  - Maliciously send any material by email that could cause distress or offence to another user.

  - Forward frivolous material e.g. chain emails, or use 'reply all' when informing the sender that they feel an email was not meant for themselves.

All Users Must:

  - When a user sets up an NHSmail account, they must identify themselves honestly, accurately and completely.

  - E-mail is to be used for the purposes of the organisation to enable information to be passed across the organisation or from one organisation to another, where a legitimate and lawful purpose exists. E-mail should be viewed with the same status as any letter or memorandum and must meet the standards of business etiquette.

  - Sign off with your name, organisation and telephone number (see Section 5).

  - Use the subject field with a few short descriptive words to indicate the contents when sending e-mails. This will assist the recipient in prioritising and aids future retrieval. Confidential identifiable information should not be used in the subject field

- Type your message in lower case. Using capital letters for full words can be considered aggressive.

- Be careful about the content - make sure it adheres to this policy.

- Maintain the conventions normally used in sending a letter by post. If you usually address someone as “Dr Smith”, do the same in e-mail. E-mail carries the same etiquette as traditional communication and also the authority of the sender.

- Users must ensure that their password and answers to their security questions for the NHSmail system are kept confidential and secure at all times. Users should immediately notify the ICT Helpdesk on 0161 716 1234 or ICTServiceDesk.PennineCare@nhs.net if they become aware of any unauthorised access to their NHSmail account.

- Email messages are increasingly a source of viruses which often sit within attached documents. NHSmail is protected by anti-virus software although occasionally, as with any email service, a new virus may not be immediately detected. If a user is unsure of the source of an email or attachment it should be left unopened and the ICT Service desk informed.

- Users must familiarise themselves with the NHSmail guidance pages which include important policy guidelines, information about known issues with the service and user/administration guides. These are all available within NHSmail: https://web.nhs.net/public/?a=s

- It is possible for email to be read and sent (in the user’s name) from an unattended PC. It is the responsibility of the user to ensure that, when leaving their PC unattended, they either:
  - Shut down the PC; or

Use the “lock computer” utility by pressing control, alt, delete together and then clicking on Lock computer.

4. SENDING EMAILS

- It is the user’s responsibility to check that they are sending email to the right recipient, as there may be more than one person with the same name or a similar name. Always check that you have the correct email address for the person you wish to send to – this can be done by checking the organisation in brackets after a person’s name in the email address (for NHSMail addresses) or be checking their entry in the NHS Directory. Where the intended recipient does not have an NHSmail account, their email address can be verified by contacting them directly or the organisation they work for via the phone.

- Users should be cautious of using auto-complete – where you type part of a name in and press enter or select a name. Ensure you have the correct person from the correct organisation.

- No confidential or person identifiable information should routinely be sent from an NHSmail account to an unsecure account (this includes all commercially available emails such as Hotmail and yahoo, and some public and private sector organisation email addresses (refer to section 8 for further details)

- All outgoing email will automatically contain an appended disclaimer stating the following:

  This message may contain confidential information. If you are not the intended recipient please inform the

  sender that you have received the message in error before deleting it.

  Please do not disclose, copy or distribute information in this e-mail or take any action in relation to its contents. To do so is strictly prohibited and may be unlawful. Thank you for your co-operation.

  NHSmail is the secure email and directory service available for all NHS staff in England and Scotland. NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and other accredited email services.

  For more information and to find out how you can switch, https://portal.nhs.net/help/joiningnhsmail

5. EMAIL SIGNATURES

- Providing your contact details within an email will help to ensure that individuals are aware of your most up to date contact details. NHSmail has a facility that enables a 'signature' to be automatically applied to each email. The following layout should be adopted:

  Your Name
  Your Job Title
  Pennine Care NHS Foundation Trust
  Your work location and address
  Telephone no.
  Mobile no. (if applicable)
  Email: e.g. your.name@nhs.net
  Fax no.
  Web: **www.penninecare.nhs.uk**

- The sign off is in Arial 10 point, and laid out as shown in the example below:

  An Other
  Information Governance Manager
  Pennine Care NHS Foundation Trust
  225 Old Street
  Ashton-under-Lyne OL6 7SR
  Telephone: 0161 716 XXXX
  Mobile: 07X4 458XXX
  Email: An Other@nhs.net
  Fax: 0161 716 XXX
  Website: **www.penninecare.nhs.uk**

- Within NHSmail, you can set up your signature by clicking on options, scroll down to Email signatures, type in your email address using the above format, tick the box 'Automatically include on outgoing messages' then click save.

- Within Microsoft Outlook (2003), you can set up your signature by clicking on tools, options, mail format, signatures, new, give a name to your signature e.g. formal or informal, next, type in your email address using the above format (you can change the font etc.), click on finish, ok, select the signature for new messages and replies then click on ok.

- Within Microsoft Outlook (2010), you can set up your signature by clicking on New E-mail, then go to 'Signature', click on the down arrow to 'Signatures' and type in your contact details.

- NB. You may need to set up your signature again if you access a different pc.

- You should not add your own images or words to your auto signature beyond that prescribed above.

- GENERIC EMAIL ACCOUNTS: Advice should be sought from the Information Governance Department regarding the use of Generic Email Accounts.

6. SHARING SENSITIVE/PATIENT IDENTIFIABLE INFORMATION BY EMAIL

- No unencrypted personal confidential data should be transferred by email unless there is a legal and justifiable purpose for doing so, appropriate authority, and the sending and receiving email addresses are secure, as described in the following paragraphs.

- NHSmail (*.nhs.net) – NHSmail is a secure national email service which enables the safe and secure exchange of sensitive and patient identifiable information within the NHS and with local/central government.

- Across the NHS –
  Between NHSmail addresses:
  .nhs.net to .nhs.net is secure
  .nhs.net to nhs.uk is not secure

- Sending to legacy secure government domains
  Emails sent to legacy secure government domains listed below will automatically be sent securely and directly to the recipient's email system:
  *.gcsx.gov.uk for local government
  *.gsi.gov.uk and *.gsx.gov.uk for central government
  *.cjsm.net and *.pnn.police.uk for Police/Criminal Justice
  *.mod.uk for Ministry of Defence

  Note the legacy local and central government email domains (gcsx.gov.uk, gsi.gov.uk and gsx.gov.uk) will slowly stop being used and then switched off completely in March 2019, as all local and central government organisations migrate to using .gov.uk email addresses for all email communication as they adopt the government secure email standard.

  If the intended recipient does not have a secure email account with one of the above domains, the new NHSmail encryption can be used (see 8.5 below)

The latest guidance for using NHS mail and secure addresses can be accessed via clicking on the following Link: https://portal.nhs.net/Help/policyandguidance

Please Note: The list is reviewed and updated as changes occur and staff should regularly refer back to the NHSmail portal to ensure their lists remain accurate. The Information Governance Team will provide updates via the monthly IG Bulletins as and when required.

- New NHSmail encryption feature

NHS Mail has introduced a new function for securely sharing personal confidential data (PCD) with non '@nhs.net' email accounts (e.g. gmail, Hotmail, yahoo etc.) that involves the recipient signing up to an encryption service to create a secure link between their email and an '@nhs.net' account.

The new encryption feature does not change the way you send e-mails to the secure e-mail addresses at 8.4, and staff should always check if there is a secure email address to send PCD to before using the guidance below.

Staff are reminded that emails containing PCD should only be sent to those with a legitimate reason for receiving the information, and that only minimal, relevant information should be shared. PCD should also not be included in the subject field of emails. The use of the Secure functionality should not be considered a routine communication channel with patients.

In order to create this link for the first time the '@nhs.net' user is required to send an email to the insecure address with [secure] in the subject field of the email. The word secure is not case-sensitive but it is essential that the word is placed in square brackets (these can be found next to the letter 'P' on a standard keyboard). It is also advisable to send the document entitled 'NHSmail Secure Receiving Function' in a separate email to the non '@nhs.net' user. First time users of this function may also find the document entitled 'NHSmail Secure Sending Function' useful. These are available from the Information Governance Department's Intranet page. Also available is a guide on how to set up a template for sending secure emails in Outlook.

When a first encrypted email is received the recipient will be asked to complete a very short sign up process to the encryption system. After doing this, the recipient will be able to read and reply to the email securely, as well as securely send and read any attachments.

From this time on, this recipient will be able to securely share PCD with '@nhs.net' email account holders as long as any email containing PCD has [secure] in the subject field.

Further information on sending and receiving secure emails to non '@nhs.net' email is available from the Information Governance Department on pcn-tr.IG@nhs.net or 0161 716 3899

- You must always use the following guidelines when sending sensitive information:

  - You should make sure that any exchange of sensitive information is part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated

- o Caldicott principles should apply whenever sensitive information is exchanged i.e.
  - Justify the purpose(s) of using confidential information.
  - Do not use patient-identifiable information unless it is absolutely necessary.
  - Use the minimum necessary patient-identifiable information that is required.
  - Access to patient-identifiable information should be on a strict need-to-know basis.
  - Everyone with access to patient-identifiable information should be aware of their responsibilities.
  - Understand and comply with the law.
  - The duty to share information can be as important as the duty to
  - Protect patient confidentiality

- o Caldicott Guardians are senior staff in the NHS and social services appointed to protect patient information. The Caldicott Guardian for the Trust is the Medical Director.

  - As with printed information, care should be taken that sensitive information is not left anywhere that it can be accessed by other people e.g. on a public computer without password protection.

  - When you are sending sensitive information, you should always request a delivery and read receipt so that you can be sure the information has been received safely. This is especially important for time sensitive information such as referrals.

  - You must not hold patient identifiable data in your calendar if your calendar may be accessed by other people who are not involved in the care of that patient.

  - If patient identifiable information is visible to other people, it is your responsibility to ensure that those people have a valid relationship with the patient.

  - You must always be sure that you have the correct contact details for the person (group) that you are sending the information to. If in doubt, you should check the contact details in the NHS Directory or by telephone.

  - If it is likely that you may be sent patient and/or sensitive information, you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected. Unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.

7. EMAILS SENT / RECEIVED IN ERROR

- If you receive an incorrectly addressed email, you should return it to the sender immediately, unless it contains confidential information, in which case you should remove this information before returning it. You should inform the Information Governance team via pcn-tr.ig@nhs.net

- Where a user sends an email containing confidential information to an incorrect address, or too much / incorrect confidential information to a person who is not entitled to receive the information, they must complete an incident form immediately.

- Where the email reasonably appears to be spam, it should be deleted without being opened or forwarded.

8. USE OF THE ‘OUT OF OFFICE’ ASSISTANT

- Use the Out of Office Assistant whenever you are unable to respond to e-mail for an extended time. Include the dates you will be unavailable and alternative contact details.
- Within NHSmail to access the Out of Office Assistant click on options, then out of office assistant on the left-hand panel.
- Within Microsoft Outlook (2003), click on tools, Out of Office Assistant, type in the ‘Auto reply only once to each sender with the following text’ box the message you require to be seen. Click on ‘I am currently out of the office’ if you require the message to be seen with immediate effect.
- Within Microsoft Outlook (2010), click on File in the top left and then click on the box headed ‘Automatic Replies (Out of Office)’

9. LOGGING ON TO NHSMAIL ON A PUBLIC COMPUTER

- One of the key advantages of NHSmail is the ability to access your email wherever you are. However, if you access your NHSmail from a public computer, it is essential you take certain precautions in order to safeguard your login details and the sensitive data in your NHSmail mailbox.

  - Make sure no one watches you type your username and password when you log in; and
  - Never select an option that allows you to save your password for later use. Always type your password, even if you plan to use the same computer for several days
  - If you are logging onto NHSmail via a smartphone or similar device, ensure you are familiar with how your phone handles NHSmail, for example ensuring that if you open an attachment, the attachment isn’t downloaded onto your device. If this does happen, you should find and delete the download as soon as you have finished your session on the email.

- Guidelines for opening an attachment

  Follow these guidelines when you open an attachment:

  - Open attachments only from people you know and trust.

  - If you are using a public computer, click the Open as Web Page link next to the attachment name. This protects you from potential virus attacks and prevents a copy of the attachment from being created and stored in the temporary files on the computer.

- o If you want to open an attachment directly rather than as a Web page, save it to a secure folder or a location that you can easily find and then open it from that location. It is not possible to open an attachment directly if you are using a public computer. Do not save documents to computer hard drives (usually known as C drives), particular when you are using non Trust issued equipment.

10. LEGAL ADMISSIBILITY

- Email is admissible as evidence in a court of law and messages can be classified as legal documents. Internal emails may also need to be disclosed under the Freedom of Information Act 2000 (contact the Trust Information Governance Team for more information about the FOI Act). Emails should be treated like any other communication and care should be taken to ensure that content is accurate and the tone is appropriate. It is an offence to delete emails after a request for them has been received.

- Emails may also be requested as part of a Subject Access Request. Subject to Data Protection rules regarding disclosure, we cannot refuse to release emails on the basis that we don’t think what was said in them was appropriate. If it’s recorded, it has to be considered for disclosure. Again, it is an offence to delete emails after a request for them has been received.

11. THE NHS DIRECTORY

- It is the user’s responsibility to make sure their details in the NHS Directory are correct and up to date.

- A user must not use the NHS Directory to identify individuals or groups of individuals to target for commercial gain, either on the user’s behalf or that of a third party.

12. COMMUNICATING WITH CLIENTS/CARERS/RELATIVES VIA EMAIL

- On occasion, it may be appropriate to communicate with clients or relatives/carers via email as this may be the preferred method that is agreed between the two parties i.e. clinician/staff member and patient/relative. This should be via a team email account rather than to an individual staff member.

- If a request to communicate via email is received and the recipient of that request does not consider it is an appropriate method of communication, the reason behind that decision must be shared with the person making the request. There is no obligation on any member of staff to communicate with clients or carers/relatives via email. However, Trust staff must ensure there is an alternative method to allow appropriate communication to take place.

- Communication via email to clients or carers/relatives will not usually be secure, unless using the new NHSmail encryption feature (see section 8.5 above), the person with whom you are communicating with should be advised of this process and agree that email communication can continue or whether they would prefer to be contacted by mail/telephone.

- When communicating with patients/relatives/carers, explicit consent of the client must be in place (see the Confidentiality Policy (CO04) and Information Sharing Policy (CO13) for further advice on consent).

- The Information Governance Team MUST be consulted before email correspondence of this nature takes place. The IG Team will provide an appropriate clause as part of the consent process.

- Any correspondence communicated by email should follow the same rules as with any other format i.e. verbal/letter, in terms of the use of appropriate content and language. The communication should be printed and retained in the appropriate record or filed electronically.

- Procedures must be put in place to ensure that, where the communication via email has been agreed, during periods of staff absence, there is an appropriate method of ensuring that emails are not left unanswered. This may be via the use of a team email account rather than to a named member of staff.

13. GLOBAL EMAILS

- High priority corporate messages/briefings to all Trust staff – Only critical or high priority messages will be circulated by global email to all staff.

- Borough-wide or service-wide messages – Staff are encouraged to develop their own local email distribution lists so that emails can be more accurately targeted. The ICT Department will be able to offer support on setting up these lists, where required and has created borough-wide and service-wide email distribution lists. However, these lists will only be made available to designated staff.

- Non-urgent messages that are relevant to all staff – For any non-urgent messages to all staff, the relevant template should be completed (appropriately approved) and returned to the Communications Department. Messages will be uploaded to the ‘Announcements’ area of the intranet within around two working days.

- Use of BCC – There are 2 ways to copy other users into an email; you can use CC (carbon copy) and BCC (blind carbon copy). CC allows all recipients of the email to see other email addresses. IF you want to copy other users in privately use the BCC field. Any recipients on the BCC line of an email are not visible to others on the email.

- For security and privacy reasons it is best to use the BCC feature when sending an email message to a large number of people. When you place email addresses in the BCC field of a message those addresses are invisible to the recipients of the email.

14. MANAGEMENT/RETENTION OF EMAIL MESSAGES AS A RECORD

- To manage email messages appropriately, members of staff need to identify email messages that are records of their business activities as opposed to routine email messages. Emails regarding clients should be printed and filed in the health record if a paper record is in use.

- It is important that email messages and their attachments which are records are moved from personal mailboxes and managed with and in the same way as other records. They should be saved to the relevant folder in the shared drive unless the information is in draft or is confidential, in which case staff should save it in their personal area on a network drive.

- All email sub-folders count towards the amount of space you are taking up, not just the mail in your inbox. It is good practice to regularly check the size of your mailbox. Look at the folders that are taking up the most space and decide whether you really need to keep all the messages in them.

  - Remember that you have primary responsibility for the emails you generate.

  - Emails are another form of a ‘record’ and are, therefore, subject to Records Management legislation and local policy i.e. the Records Management Policy (CO20).

  - You must never delete email (or any other type of record) if you know it is subject to a Freedom of Information Act or Data Protection Act request that has been received by the Trust. This act would constitute not only Trust policy breach but also breaking the law.

15. MONITORING AND DISCLOSURE OF EMAIL

- As outlined in the Regulation of Investigatory Powers Act (RIPA), the Trust reserves the right to access and disclose the contents of electronic communications without the explicit consent of the user (only to the extent that it will not contradict relevant clauses in the Human Rights Act). The Trust will do so when it believes it has a legitimate business need and only after explicit authorisation from an Executive Director.

- Reasons for monitoring and disclosure may include but are not limited to:

  - Provide evidence of sales orders, invoices or other business communications.

  - Absence (e.g. due to sickness, holiday or business commitment) where there is a need to access messages in order to carry out the normal functions of the Trust.

  - To further an investigation triggered by indications of misconduct or unauthorised use: or, upon production of evidence, to ascertain whether the law has been broken

- You should have no expectation of privacy for any personal email that you send or receive via the NHSmail service.

16. PERMITTED USE OF THE TRUST INTERNET FOR PERSONAL EMAIL USE

- Use of the Trust internet is permitted to enable users to send personal emails provided that the user sets up their own personal account with an internet provider. Use must not be detrimental to the individual's job responsibilities, be in their own time and not stop other staff members using Trust equipment to carry out their duties. The same procedures and restrictions apply as outlined within this policy.

- The Trust can accept no responsibility for any matter arising out of personal use of email and cannot offer support for any problems encountered.

- Users who give out home phone numbers, addresses, credit card numbers, financial or other confidential information do so at their own risk.

- Personal use of Trust equipment does not extend to the printing of large documents. The cost of consumables is expected to be borne by the user.

17. REPORTING AND MONITORING MISUSE OF EMAIL

- Any misuse of the email system or violations of this policy must be notified to the user's line manager and/or the Trust ICT Director immediately. The Trust may, with reasonable suspicion of Policy breach occurring, initiate monitoring of staff email usage and accounts.

18. TRAINING

Ad-hoc training may be available from the Information Governance team on request.

19. 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

20. 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.

21. 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.

22. SAFEGUARDING

All staff have a responsibility to promote the welfare of any child, young person or vulnerable adult they come into 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.

23. 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.

24. 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.