ELECTRONIC COMMUNICATIONS AND INTERNET ACCEPTABLE USE PROCEDURE

Document Reference	Proc451 (IG)
Version Number	4.1
Author/Lead **Job Title**	Karen Robinson Information Governance Officer
Lead Director name	Peter Beckwith, Senior Information Risk Owner and Director of Finance
Consultation	Information Governance Group
Date of Last Changes (This Version)	15 May 2024
Date of Next Review	May 2027
Name of approving group **Date of approval**	Information Governance Group 15 May 2024

VALIDITY – Procedures should be accessed via the Trust intranet to ensure the current version is used.

CHANGE RECORD

Version	Date	Change details
Policy P010 Electronic Communications and Internet Policy		
4.11	*12/12/2005*	
4.12	*03/10/2011*	*Addition to 5.4.5. Update to the policy summary in Appendix 4*
4.14	*1/10/12*	*Introduction expanded to include all messaging systems Section 5.5 added regarding the use of SMS to contact patients – approved IG Committee 18 July 2012*
5.00	*Aug 2014*	*Reviewed with major changes: Update to Section 5.2, policy restructured into specific sections on: Personal use of social media, Business use of social media, communicating with a patient via text or email and Communicating with a patient via trust mobile telephone. Section on the use of SMS text for appointment reminders updated. Additional consent form added in Appendix 2. Appendix 3 Consent form updated.*
5.01	*March 2015*	*A section on the Business use of online meeting services added. Policy reviewed to incorporate move to NHSmail.*
5.02	*October 2015*	*Requirement to password protect removed, Monitoring section updated*
Dec-16 Policy transferred into Electronic Communications and Internet aAcceptable UIse Procedure (Proc416(IG) from Electronic Communications and Internet Accetable Use Policy (P010)		
1.0	*Nov 2016*	*5.3 updated in relation to new guidance from NHS protect re social media attacks on patients. 5.9 updated in relation to consent for text reminders.* *Further amendments made before formal ratification.* *5.4 updated to provide guidance to staff accessing online professional discussion groups. 5.5 updated regarding the approval process. 5.8 updated to remove the need to use the read receipt mechanism and to remove the need to keep items for no longer than 3 mths. 5.8.1. updated to re-instate the process for delegate access for managers during times of unplanned absence. This function is now available in NHSmail2. 5.8.6 added to allow access to NHSmail from non-Trust mobile devices. 5.8.7 added to allow access to non-Trust email accounts on Trust mobile devices if there is a business need. 5.9 updated in relation to consent for text reminders. 5.10 and Appendix 3 consent form updated regarding the use of encrypted/pin code mobile phone to text patients and giving patients the option of having email encrypted. 5.12 updated to remove the need to comply with internet and intranet site terms and conditions. 5.13 and 5.14 update to remove the responsibility from employees to check that virus protection is installed on their pc. 5.14 updated in terms of employee agreement for complying with the policy when working remotely.*
1.1	*Feb 2018*	*Update 3.4 re approval of social media accounts for individual teams. Further update to 3.8.5 re: [secure] email. Update 8.1 for the authorisation necessary for accessing emails for investigation purposes.* *Further amendments from IG Group. Manager to keep social media accounts up to date and for the Strategic Comms Manger to maintain a list and regularly review. Removal of secure government email addresses and the Secure File Transfer service.*
1.3	*Sept-18*	*Update references to recent data protection legislation.*

2.0	February 2019 March 2019	Full review – major amends Section 3.5 add that staff must ensure information stored on cloud services is available to those who need it for operational purposes. For staff to confirm to IT that cloud storage is not being used for personal/business sensitive information. To remove the requirement for requests to be authorised by a senior informatics managers. To clarify that data must not be backed up to non-Trust approved cloud services. To add that SIRO must approve the use of cloud services for the storage/transfer of personal data, ensuring that the requirements NHS Digital Cloud Risk Framework are met. Update 3.5 in respect of NHSmail Skype for Business and instant messaging within NHSmail. Update 3.8.1 to include bcc function. Update 3.8.3 to include shared .pst files on the O drive. Add links to NHSmail encryption guidance in 3.8.5. Update 3.14 in relation to download attachments, not to save passwords in browsers and VPN connectivity on Trust laptops. Add in link to NHSmail Access to Data Policy. Additional amendment via email and verbal confirmation at March IG Group. Section 3.8.5 updated with the NHSmail change in policy for sending secure emails.
3.0	September 2020	Reviewed – Major amends Removed the sections on personal and business use of social media as these are now included in the social media policy. Updated the section on Online meetings to reflect the applications currently being used by the Trust. Added further information regarding the recording of such meetings. Minor updates to Instant Messaging section to refer to MS Teams. Further housekeeping guidance added in relation to saving emails and managing group mailboxes. Sending personal data by email updated to the last NHSmail guidance. N3 definition removed.
3.1	January 2021	Additional bullets and changes to Section 3.4. Agreed virtually November 2020 Section 3.7.5 to include the ability to revoke emails sent [secure] and further bullets regarding attachments. Agreed virtually January 2021.
3.2	March-22	Reference to fax removed at section 1. Inclusion of MS Teams in section 3.2. Specify section 3.3 relates to third-party online collaboration tools. Downloading MS Teams recordings and restriction settings for virtual meetings at section 3.4. Inclusion of mailbox owner notification when delegate access granted by local administrator in 3.7.1. Addition of email archive and removal of reference to pst file on O drive and update hyperlink to the Records Management Code of Practice 2021 to section 3.7.3. Added section on Egress to section 3.7.5 and that breaches should be reported on datix. Update 3.11 to direct requirements for intranet/internet sites to the Communications Team. Updated 3.13 to define remote working using Trust supplied equipment and non-trust supplied equipment. Updated 8.1 to include accessing NHS mail for SARs to include NHS Digital introduction of automatic notification when granting access to a user's emails. Approved at IG (Information Governance) Group on 09/03/2022. Template formatted and updated back to procedure template by policy management and version numbers corrected as per previous versions
3.3	October 2022	Section 3.4 update to advise that recordings can be made for minute taking purposes and deleted once the minutes are approved.
4.0	October 2023	Full review of procedure. Section 3.3 updated to include sharing documents via SharePoint/One drive and to remove the need for sharing business sensitive information via other cloud storage sites. Section 3.5 updated to regarding record keeping of Instant messages. Section 3.7.1 updated regarding the availability of MFA and what to do if any email has been received or sent in error. Added 3.7.2 in relation to sending bulk emails and when to use bcc and email merge. Updated 3.7.9 in line with the latest Safe Haven Procedure for storing data in Outlook Calendar. 3.8 updated in line with NHS Transformation Guidance on text messages and recording patient preferences. 3.9 updated to regarding documenting emails. 3.13 updated on working remotely to include the use of a screen protector, not leaving equipment and not allowing others to use your device. 6.1 process of subject access requests for emails amended. 6.2 added in relation to access staff mobile phones during absences. Appendix 2 consent form updated. Appendix 5 updated to remove reference to pst files. References updated to UK GDPR. Approved at IG (Information Governance) Group on 04/10/2023.
4.1	May 2024	3.4 Added reference to SharePoint. 3.7.1 Changed name of Out of Office Assistant to Out of Office Automatic Reply. Changed the time an NHS Mail account is deleted from 6 months to 90 days. (NHS England policy. Deleted bullet referencing MFA for new users of NHS Mail as MFA enabled for all users. Added bullet regards enabling delivery/read receipts if sending urgent/critical emails and use an alternate contact method to confirm receipt. 3.7.2 Added bulk email autodetect and blocking of email accounts. 3.7.4 Changed Group Inboxes to Shared mailboxes. 3.7.5 updated reference to Trust Brand Centre. Approved at Information Governance Group (15 May 2024).

Contents

1. INTRODUCTION

At Humber Teaching NHS Foundation Trust communication plays an essential role in the conduct of our business. The Trust values employees' ability to communicate with colleagues, clients and business contacts. How an employee communicates with people not only reflects on themselves as an individual but on the Trust as an organisation. This procedure sets out clear rules for the use of the Trust's email, internet, , land line, mobile phone or system messaging facilities.

The organisation trusts its employees to use the information technology and communication facilities sensibly, professionally, lawfully, consistently with an employee's duties, with respect for other employees and in accordance with this procedure and the Trust's rules and policies.

Any inappropriate use of the Trust's communication systems whether under this procedure or otherwise may lead to disciplinary action being taken against an employee under the Trust's disciplinary procedures which may include summary dismissal.

The Trust reserves the right to withdraw from individual employees or groups of employees the facility to send and receive personal communications by particular methods. For example, abuse of the email system may result in the withdrawal of the right to use email for personal correspondence.

The Trust expects all employees to have access to email and to have their own work email address. Access to email can be obtained by contacting the Humber IT Service Desk.

This procedure supports the Information Security and Risk Policy

2. SCOPE

This procedure applies to all employees of the Trust, including all staff who are seconded to the Trust, contract, voluntary, temporary and agency staff and other people working on Trust premises. This includes members of staff with an honorary contract or paid an honorarium.

3. PROCEDURES

The Trust's procedure on the acceptable use of electronic communications and internet is:

3.1. Inappropriate Use

It is strictly prohibited to use communication technology to create, access, download or transmit any:

- Defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.
- Material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people, as detailed in the Bullying and Harassment Policy.
- Pornographic images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- Any copyrighted material in a manner that violates that copyright.
- Any material for the purpose of corrupting or destroying the data of other users.
- Junk mail or spam.

Employees must not take private film or photos, whether on phone cameras or otherwise, of patients in your care.

3.2. Personal Use of Trust Communication Facilities

Although the Trust’s communication facilities are provided for the purposes of Trust business, we accept that the facilities may occasionally be used for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this procedure are complied with.

Employees must ensure that email, internet, collaboration tools (e.g. MS Teams) and telephone systems (including mobile telephones) are not used excessively for personal use. This includes personal devices. Personal use must:

- not interfere with the performance of their duties
- not take priority over their work responsibilities
- not incur unwarranted expense or liability for the Trust
- not have a negative impact on the Trust in any way
- be lawful and comply with this procedure

Examples of personal use which breach these requirements include:

- Streaming media over the internet
- Making international calls using Trust telephone or mobile telephone
- Using the internet for personal use during working hours
- Signing up to automated emails from organisations/companies for personal use
- Downloading large amounts of data to mobile devices, e.g. smartphones for personal use
- Forwarding emails in the form of chain letters, junk mail, jokes and emails containing dynamic information (video clips, macros, software etc.)

Staff must note that whilst personal use of the communications system is permitted:

- Staff must not use the communication systems for personal business/commercial purposes, e.g. renting out your holiday cottage
- Staff will meet the cost of personal calls and texts from Trust mobile and landline telephones
- The Trust does not accept any responsibility for personal emails that are delayed, incorrectly quarantined, detected as spam, or are not received by you
- The Trust does not accept any responsibility for personal data you divulge about yourself, e.g. fraudulent emails sent by hackers requesting banking details
- Staff should mark personal communication “Personal” in the subject line
- Absolute privacy cannot be expected because the Trust may need to monitor communications for the reasons set out in Section 8

3.3. Business Use of Third-Party Online Collaboration and Storage

Secure online collaboration is available using N365 SharePoint and OneDrive. Documents should only be shared with those who have a need to know and removed when no longer required Users must ensure that access and security permissions are regularly reviewed and updated. Documents must be retained in the appropriate records management system in accordance with the NHS Records Management Code of Practice.

Staff may access and share information using other online collaboration tools providing that it does not contain any personal data or business sensitive information. The Trust cannot guarantee the security of such sites so the information stored on such sites must be of the quality that would not breach the Data Protection Act 2018, UK General Data Protection Regulation, Common Law Duty of Confidence or bring the Trust in to disrepute if a security breach occurred. Staff must ensure that the information is available to those who need it for operational purposes.

In order to gain access to such services a request must be made by email to the IT Service Desk detailing the name of the site/service and the business need for access and confirmation that it is not being used for personal/business sensitive information. The request must be supported by the user's line manager or other appropriate senior manager. The supporting manager must ensure that the user has completed their information governance training, be sure that no other Trust/NHS system is more appropriate, and both the user and manager must understand the risks associated with accessing such sites/services.

IT Services will verify that the site is safe and appropriate for business use and if necessary, request further information for audit purposes from the user or their supporting manager.

Granting access to facilities such as cloud storage (e.g. Dropbox) may also give access to other facilities such as web mail (e.g. Gmail, Outlook.com) and vice versa. If it is necessary for business purposes, web mail may be used to receive non-confidential and non-business sensitive information. However, staff must use Trust email accounts for any emails sent in relation to Trust business.

Trust devices must not back up or store data to non-Trust approved cloud services.

3.4. Business Use of Online Meeting Services

Secure online meeting services are available for staff to utilise for teleconference and web conferencing (including video conferencing), using NHSmail's MS Teams, Upstream and GoToMeeting (for group therapies). Patient information and business sensitive information may be discussed and shared using these methods providing that the below requirements are met:

- Existing professional standards and Trust policies for confidentiality and record keeping must be followed; as for current face to face meetings.
- Only Trust encrypted devices should be used to access online meeting services. However, MS Teams can be used by both Trust and personal devices using your NHSmail credentials.
- Documents containing patient information or business sensitive information may only be shared via screen sharing and must not be uploaded on to the online meeting service.
- Unless required for the meeting, participants should close down clinical systems and other screens containing confidential/business sensitive information. This will avoid the chance of inadvertently screen sharing confidential information.
- If it is necessary to record a meeting for minute taking purposes, the recording must be made and stored in line with the Trust's Photographing, Video and Audio Recording Procedure. MS Teams meeting recordings are stored in OneDrive (under Files-> OneDrive -> Recordings), and any recordings made should be downloaded from this location to a secure location (such as the V: drive or SharePoint) and deleted as soon as the minutes have been approved.
- If the meeting will result in a significant change to clinical process or clinical ways of working, the Clinical Safety Officer must be consulted, and the clinical safety considerations documented.
- When organising virtual meetings via MS Teams, a new meeting request must be created for each date that this meeting will be held. The use of recurring meetings in MS Teams will give any attendees who previously attended that meeting access to future dates and any chat or recordings associated with that meeting. Further restrictions are also available in *Meeting Options* within the appointment to restrict the chat availability to 'in meeting only' or disable it altogether if appropriate.
- Take reasonable measures to ensure that personal/business sensitive information cannot be overhead. This includes the use of headsets to minimise information being overheard and ensuring doors are closed when initiating/receiving a video call. When in Trust buildings, use signs/notices on doors to indicate that a meeting is taking place.

Meeting organisers must ensure that:

- all attendees at the meeting have a "legitimate relationship" with the patient.

- attendees are invited using secure email, e.g. NHSmail.
- attendees are invited to the correct meeting and verify prior to sending to the invite.
- the correct participants have joined the meeting.
- participants are in a secure location if personal information or business sensitive information is being discussed.
- meeting permissions/settings are considered so that meeting participants can be admitted as appropriate. These should be set at the time the meeting is organised.
- a privacy statement is issued at the start of the meeting – detailing who you are, what you are going to do with the information, who will have access to it and why.

When using video conferencing for patient consultations, staff should follow the Standard Operating Procedure Patient Video Consultations.

Online meetings initiated by other organisations using other software may be joined using the web version rather than downloading an application. Personal/business sensitive information must not be shared using this software unless a Data Protection Impact Assessment has been signed off by the Trust. The Information Governance Team should be contacted in the first instance.

3.5. Instant Messaging

Instant messaging (IM) using NHSmail's MS Teams is secure and may be used to exchange patient/personal or sensitive information. An instant messaging conversation should be treated in the same way as a telephone conversation or email; after discussing any patient information via IM, staff must properly document a record of all relevant conversations within the patient health record. Section 3.7 Use of NHSmail also applies to any communications using IM.

Other IM applications (e.g. WhatsApp) may only be used for non-personal data/business sensitive information unless agreed with the Trust.

When using these applications for work purposes staff must:

- Not allow anyone else to use the device
- Set your passcode immediately and for it to lock out after a short period of not being used.
- Disable message notifications on the device's lock screen
- Enable the remote-wipe feature in case your device is lost or stolen.
- Ensure you are communicating with the correct person or group.
- Take care when selecting the membership of a group and review the membership regularly.
- Keep social groups and work groups separate.
- Keep a record of any IM needed for future reference in the appropriate records management system.
- Delete chats when no longer required for the purpose.
- Remember that instant messages can be subject to Information Requests.

3.6. Viruses

Viruses can damage computer systems, destroy data, cause disruption and incur considerable expense for the Trust. Employees connected to the network must have an appropriate virus scanner on their computer which is regularly updated.

Employees who suspect a virus may be attached to a file downloaded from the internet or attached to an email must inform the IT Service Desk immediately on Tel. 01482 477877 or email hnf-tr.itservicedesk@nhs.net. This must also be reported via Datix as an adverse incident (please refer to the policy on our Intranet).

Employees must not load software onto their computers before first seeking advice/agreement from the IT Service Desk.

3.7. Use of NHSmail

3.7.1. General rules

Care must be taken when using email as a means of communication as all expressions of fact, intention and opinion via email may bind an individual and/or the Trust and can be produced in court in the same way as oral or written statements. Electronic messages are admissible as evidence in legal proceedings and have been used successfully in libel cases. A comment made in jest on email can be misinterpreted. Email is non-interactive, and you do not have the advantage of voice inflection or body language. In the case of harassment it is the effect of the communication which is considered and not the intention of the sender.

All emails are accessible to the public under the Freedom of Information Act 2000 unless they are subject to one of the exemptions. Further information about the Freedom of Information Act 2000 is available on our Intranet site under ‘Policies and Procedures’.

When using email, staff must follow the following principles:

- Whenever staff are away from the office for 24 hours or more, an “Out of Office” Automatic Reply must be used detailing the date of return and an alternative contact.
- During unplanned absences, line managers may have access to their member of staff’s email for a maximum of five working days. This must be authorised by the Head of Service, via email to the IT Service Desk. During this time, manager must make alternative arrangements to ensure business continuity, for example through the use of the “Out of Office” Automatic Reply. Managers must not access emails marked “Personal”. Managers must only open emails marked “Confidential” when absolutely necessary, e.g. for patient care. An email notification will be sent automatically to the mailbox owner when access is both granted and revoked. It is good practice to inform the staff about the reason for this on their return.
- Emails may only be set up to be automatically forwarded to email users within NHSmail. Employees using this rule must ensure that personal data received via email is not forwarded to other employees who do not need to see it.
- Employees must not impersonate any other person when using email or amend any messages received.
- Ensure that when replying to an email that has been sent to many recipients that you reply to the sender and not “Reply all” unless it is necessary that all recipients receive the reply.
- Do not open emails or attachments from unknown sources. These must be deleted without opening.
- Web mail (e.g. Gmail, Outlook.com) must not be used for Trust business.
- Access NHSmail on a regular basis. NHS mail accounts will be marked as “Inactive” if an email is not sent from the account every 30 days. Accounts will be deleted if not accessed for 90 days.
- If you are not the intended recipient of an email, delete the email from your inbox and deleted items and notify the sender.
- Re-call any emails sent in error immediately. Please note that emails sent outside of NHSmail cannot be re-called, unless sent via Egress. A Datix must be submitted if the email contained business sensitive/personal data and re-call was not successful/email read by recipients. In such circumstances, ask recipients to confirm deletion from their inbox and deleted items.
- If you are sending an urgent/critical email you must enable read/delivery receipts and contact the recipient by an alternative method to confirm they have received the emails.
- Take care when using Contact Groups, ensure that the Group is clearly named and that members are reviewed and updated prior to use.
- Do not use Contact Group for patients/client/volunteer contact details. Contact details may be held on a distribution list which is regularly reviewed and updated.

3.7.2. Bulk emails

When sending emails to multiple recipients the following security measures should be followed:-

- Emails sent to all staff should be submitted to the Communications Team for circulation.
- The use of “To” field and “cc” field (carbon copy) can be used when all the recipients are known to each other, for example an internal email and it is useful to inform recipients that others are aware of the email.
- The use of the “bcc” field can be used when sending non-sensitive information internally and you would like to avoid “reply all” responses.
- An email merge should be used when sending an email to a number of external recipients such as a group of patients, volunteers etc. This will ensure recipients are not made aware of other recipient’s email addresses. A separate email will be sent to each person on the distribution list avoiding any potential IG breaches. The following guide explains how to Use mail merge to send bulk email messages - Microsoft Support. The email will be sent from the user who setup the mail merge. Email merge messages cannot be sent from a shared mailbox.
- If you ignore the above and send bulk emails, NHS Mail will detect this and will automatically block your email account, and reset your MFA and password.

3.7.3. Disclaimer

The below disclaimer must automatically be attached to all outgoing emails. This is designed to limit the Trust’s potential liability with respect to information being communicated. The disclaimer, however, is not meant to preclude the user from undertaking fundamental checks before sending the email including checking the content for accuracy, correct addressee, etc.

> *This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you are not the intended recipient you are notified that any use, disclosure, copying or distribution of the information is prohibited. In such cases you should destroy this message and kindly notify the sender by reply email.*
>
> *All emails will be scanned by the Trust for viruses, spam and malicious content. However, Humber Teaching NHS Foundation Trust will not be liable for any losses as a result of any virus contained within this email or attachment(s). We are not liable for any opinions expressed by the sender where this is a non-business email.*
>
> *If you do not receive the entire message, or if you have difficulty with the transmission, please telephone us immediately.*

3.7.4. Housekeeping

To help with speed and efficiency of email, it is important that staff adhere to the housekeeping rules outlined below:

Inbox/sent items

The amount of email kept in the users Inbox/Sent Items must be kept to a minimum and emails must be deleted or online archive after reading, response or action. NHSmail has mailbox size limits. You will receive warning emails as you approach your limits. If this happens you need to delete or archive your email as soon as possible. If you go over your limit your mailbox will eventually restrict your ability to send/receive mail and to send meeting invitations.

Permanent storage

Professional Code of Conduct and Trust policy requires health professionals to keep clear, accurate and legible patient records. It is important that emails do not hinder this. You should ensure that relevant data contained in emails is immediately attached to the patient record. Failure to do so could have implications on patient safety.

Under the Freedom of Information Act the Trust is required to be open and transparent in the conduct of its business. In order to do this emails must be saved if they contribute to the full understanding of a decision; result in action being taken; or forms a significant part of the story. If not, they must be deleted.

Emails that need to be saved must be saved in an appropriately titled folder on the Trust network, such as the V: drive or SharePoint in line with the Records Management Code of Practice 2021

It is not necessary to save every reply within the email conversation. Emails should only be saved at significant points in the conversation or when they include attachments that contribute to the decision, action taken or story.

Email Archive

As NHS Mail no longer supports PST files, every NHS Mail account now has an Online Archive folder available. Regardless of the mailbox size, this folder is 100 GB, and allows every user to move emails which need to be retained long term to be moved to this folder. This folder is also searchable within NHS Mail and all emails stored in it are easily accessible.

Deleted items

Emails that are deleted from the user's Inbox automatically transfer into the Deleted Items box and must be deleted on a regular basis in order to free up storage space.

Shared mailboxes

The same housekeeping also applies to group mailboxes. Shared mailboxes must not be used to store emails. Emails must be deleted as soon as possible or moved to a secure location (such as the V: drive or SharePoint) and deleted as soon as possible.

Email address book

Staff must keep their entry in the Directory up to date. The entry must provide information such as location, address, telephone number, job title and department. This will ensure the correct identification of the email recipients, particularly if there are multiple people of the same name.

3.7.5. Etiquette

The following points provide guidance on etiquette when corresponding via email:

- Only use upper case letters when it is appropriate for correct grammar, some people consider emails written solely in CAPITAL letters to be aggressive.
- The subject field must always be used to add a short description of the contents of the email. This will assist the recipient in prioritising opening of email and aids future retrieval of opened messages.
- The importance and sensitivity flags must be used as appropriate. This will assist the recipient in prioritising opening of email.
- Care must be taken with content. Nothing must be written in an email that would not be written in a letter or said to someone face-to-face. Business and personal emails must be kept separate – do not mix content of emails. Email content may be requested under the Freedom of Information Act 2000.
- The use of words must follow our NHS values and principles and be professional, clear, respectful, accessible and straightforward and written in Plain English.
- The same conventions should be used as when sending a letter by post, e.g. using the same style of salutation (yours sincerely, etc).

- Emails must be signed off with the name, title and contact details of the author using the standard Brand centre guideline. This can be added to a signature file so that it appears automatically and includes a disclaimer.
- Emails must be treated as post and opened, where possible, on a daily basis.

3.7.6. Sending personal data/business sensitive information by email and instant message (IM)

NHSmail provides of secure way of sending personal data/business sensitive information to other NHSmail users by email and instant messaging, including MS Teams. It is one of a number of government secure email systems. It connects securely to all of them allowing NHSmail users to share information confidently and securely with their users.

Emails can be sent securely to the following domains without any further action or protection, other than ensuring you have correct recipient:

- nhs.net
- gov.uk (no longer needs to be gsi.gov.uk, gcsx.gov.uk)
- cjsm.net
- pnn.police.uk
- mod.uk
- parliament.uk
- a domain accredited to DCB1596 Secure Email Standard https://digital.nhs.uk/services/nhsmail/the-secure-email-standard(click here for list)

If sensitive information needs to be shared with a non-NHS Mail email address, staff should use Egress (enabled by including '[secure] in the subject line), or using the Egress plug-in for Outlook. Egress requires the recipient to register and create an account to be able to retrieve the files, and has the added advantage that i) the email and attachments are securely held within the Egress application, so are never actually 'sent' to the recipient, ii) it has a tracking feature which shows whether a recipient has accessed the email, and iii) has a 'revoke' feature which can be used to remove the previously sent email (effectively a 'recall' feature).

All personal data/business sensitive information sent outside of these domains should be sent using Egress by including [secure] in the subject heading, or by using the Egress Outlook plug-in. This includes email sent to nhs.uk and nhs.scot email addresses.

Before using the Egress:

- Ensure that the recipient is expecting it and ready to handle the contents appropriately.
- Send the recipient the Accessing Encrypted Email Guide for non-NHSmail users so that they can register for the service.
- Send an email to the recipient with [secure] detailed in the subject heading via, or by using the Egress plug-in for Outlook. At this stage, the email should not contain any personal/business sensitive data. The recipient will then be prompted to register with the encryption service.

Once the recipient has confirmed registration via an encrypted reply, personal data/business sensitive data can then be emailed. The email must still have [secure] in the email heading. Further information can be found at Encryption Guide for NHSmail.

This method should also be used when communicating by email with a patient/advocate. This must be with the explicit consent of the patient, see Section 3.10 Electronic Communications and Internet Acceptable Use Procedure.

Any breach of confidentiality resulting from using email for personal identifiable data will be investigated and you are responsible for showing why any of the following guidelines may have not been applied. Messages containing personal data sent to the wrong recipient will be classed as a breach of confidentiality even if it is another NHS employee. Breaches should be reported on Datix immediately. It is possible to revoke access to an encrypted email sent using [secure] by following the Encryption Guide for NHSmail and changing the message status from “Active” and “Revoked”.

Security measures

- Make sure you have the correct recipient. If you are unsure, send a test email or ask the recipient to email you before sending any personal data.
- Mark the message appropriately in the subject line, e.g. “confidential” or “business sensitive” and select “confidential” in the Sensitivity section in the Message Options.
- Limit the number of recipients of the message to as few as possible.
- Limit the amount of data to only that which is needed for the purpose it is being sent, e.g. use a unique identifier or initials instead of the person’s name.
- Manually select recipients from the address book and confirm their identity by checking the properties.
- Change the address book view to the Humber Teaching NHS Foundation Trust address list. This will avoid the chance of sending an email to another employee in another NHS organisation with the same name.
- Send to email addresses that are person specific unless the email can be dealt with by any member of the team reading the email. Be aware that email can be forwarded by the initial recipient to third parties against your wishes or by accident.
- Include a note to say that the receiver of patient identifiable data is responsible for the security and confidentiality of that data and must not pass it on to anyone else, via any method, who does not have a justified ‘need to know’.
- Where there is a more formal method for the communication of information, such as a web-based referral system, then that must be used.
- If you allow ‘delegate’ access to other people to your inbox, consider whether they need to see any personal data you receive.
- Anonymised information can be sent to non-secure email addresses, see Glossary of Terms for definition of anonymised.
- When in receipt of personal data remove it from your email system as soon as possible and file it appropriately, either electronically or on paper.
- Review any attachments and make sure all are relevant to the recipients. Attachments containing confidential information not intended for disclosure should be sent separately from general attachments intended for dissemination.
- The file name for confidential attachments should include the word confidential at the beginning.

3.7.7. NHSmail on non-Trust mobile devices

The Trust permits non-Trust mobile devices to be configured for NHSmail providing that the staff member is clear that they have a personal responsibility to ensure that:

- care is taken to use correct email account at all times. Sending Trust personal/business sensitive data using a non-Trust email account is a breach of this procedure
- the device is capable of being encrypted at rest. Mobile configuration guide for NHSmail provides information on devices that meet this requirement. Devices that do not have this feature must not be used
- a password protected screen saver/screen lock activates automatically after a period of no more than 10 minutes of inactivity
- Trust documents are not saved to the device
- the device is not left unlocked when unattended
- the device is not shared with others unless the device supports multiple independent accounts
- a report is made to the IT Service Desk if the device is lost or stolen

- the device is wiped remotely, using NHSmail, if lost/stolen or instructed by the IT Service desk
- the device is not set to backup emails using cloud services

Staff should be aware that devices will be remotely wiped of all data after eight failed password attempts.

Important: Devices that are remotely wiped will be restored to its default factory settings. This will wipe all data stored on the device (including any photographs and documents).

IT Service Desk does not provide IT support for personal devices connected to NHSmail.

3.7.8. Non-Trust email accounts on Trust mobile devices

Trust mobile devices are permitted to be configured for non-Trust email accounts providing that there is a business requirement. The request must be submitted by email to the IT Service desk detailing the rationale for the business requirement. Such requests must be supported by the user's line manager or other appropriate senior manager and authorised by a senior informatics manager.

3.7.9. Calendar

Personal/business sensitive information must only be stored in your Outlook calendar if access is restricted to those who need to know this information. Only the minimum personal data should be used e.g. for a nurses appointments just the name or initials of the patient and the postcode if required. Consider marking entries as private, if not, all your delegates will have to the personal data in the entry.

Outlook Calendar should not be used as a replacement for a health professional's diary. If an entry is accidently deleted from Outlook, there is no way to recover this information. Appointment details must be held in the relevant clinical system or a paper diary that is retained for 8 years.

By default, Calendar Properties is set to show only free/busy times to other users of NHSmail. As this includes users outside of the organisation, this setting should not be changed to allow access to title, locations or all details of calendar entries

3.8. System-Generated Appointment Reminders and Other Notifications via Text or Email

SMS or text messaging can be used to send patients non-sensitive personal data such as appointment reminders by text.

- Only Trust IT systems or NHSmail can be used to send SMS messages for appointment reminders and other notifications.
- Trust issued or personal mobile phones must not be used to send bulk SMS messages for appointment reminders and other notifications.
- Implied consent for confidentiality purposes can be used when contacting patients about their care.
- Services should be clear to patients about what information will be sent by text/email.
- Record the patient preference in their electronic health record and ensure that this is respected. This should be recorded at the time the mobile phones/email address is recorded.
- Patient preference can be recorded using the consent form in Appendix 2, verbally during a contact with the patient, obtained as part of the referral or as an opt-out to the text service offered by letter.
- If the patient requires emails to be encrypted, this must be recorded on the electronic record and their preference respected by using the NHSmail encryption feature. See 3.8.5.
- Appointment reminders should be in following format:

  Appointment Reminder: DD/MM/YYYY at HH:MM at Clinic Location
- The minimum amount of personal data should be communicated via email/text. For example, do not include patient details or clinic details in an appointment reminder.

- External providers of text messaging services must not be used without further approval from the Senior Information Risk Owner.
- The patient can update their preference at any time by speaking to the health professional. The health professional must update the system as soon as possible.
- Emails for groups of patients must be done using a Trust automated messaging system or using the email merge option in Microsoft Word. This will ensure that the email is individual to the patient. Emails must not be sent to groups of patients with addresses identified in the “To” field. This also applies to emails sent to non-patient groups which would reveal personal data about the recipients.
- Staff should confirm the contact details at each consultation if email and/or SMS messages are used to contact patients to ensure the details remain current.

3.9. Communicating with Individual Patients via Text or Email

Sometimes a patient may wish to communicate with the Trust via text or email. It is important the explicit consent of the patient is gained prior to communicating in this way. The form in Appendix 3 should be used. The completed form must be held in the manual record or scanned into the electronic health record.

If the patient requires emails to be encrypted, this must be recorded on the electronic record and manual record and their preference respected by using the NHSmail encryption feature (see 3.7.5).

Text messages sent and received must be documented in the patient’s notes detailing text, telephone number, time, response, any appointment made and/or referral to other agencies, date and signature of nurse.

Emails sent and received must be stored in the patient’s electronic or manual record. This can be a copy and paste of the full message or a summary of the email.

All messages must be deleted from the handset after documentation. This should be done within 24 hours to ensure that the data held on the device is at a minimum.

Only Trust encrypted devices may be used to receive and send email messages to patients using NHSmail.

Only a Trust encrypted smartphone or PIN (personal identification number) coded Trust mobile phone may be used to send or receive text messages.

Patient contact details may only be stored on a Trust encrypted smartphone or a PIN coded Trust mobile phone. The minimum data should be stored to enable the correct identification of patients, e.g. surname/initial and mobile phone number.

Avoid using identifiers of the patient or service within the text message in case the message is seen by someone other than the intended recipient.

Only send messages to the phone number/email address provided by the patient/carer to which they have consented to the Trust using. No other phone number or email address should be used.

Messages should be written in full without using “text-speak” or abbreviations.

Clarify any abbreviations or “text-speak” used by the patient, make no assumptions.

Always respond to message within an agreed timescale where relevant.

Mobile phones must be locked away when not in use.

3.10. Communicating with Individual Patients via Trust Mobile

Trust mobile phone may be used to make verbal calls to patients. Staff must:

- Use the voicemail facility to record an out of office message when they go on annual leave and provide an alternative contact number.
- Personal (non-work issued) mobile phone numbers must not be given to the patient.
- Information received via voicemail message must be treated as any other information and transferred to the patient’s health record.
- Mobile phones must be locked away when not in use. The mobile phone should have a passcode known only to the named user or practitioner.

3.11. Use of Internet and Intranet

Only software approved by IT Services can be downloaded from the internet, even if this software does not require licensing.

The Communications Department, in conjunction with all other Trust departments, shall determine the content of Trust intranet and internet web sites. Any requirements for intranet/internet sites must be directed to the Trust Communications team.

Written consent must be obtained from the individual concerned before placing personal data on the Trust’s internet site.

3.12. System Security

Employees are not to use Trust IT systems in any way that may damage, overload or affect the performance of the system or the internal or external network. The Trust’s Code of Conduct for employees in respect of Confidentiality and Information Security must be followed. In particular, employees must:

- Keep all confidential information secure, use it only for the purpose intended and not disclose it to any unauthorised third party.
- Keep passwords safe and do not share.
- Log off/lock the PC when you leave your work area.
- Store personal data/business sensitive data in a secure folder on the Trust fileservers/Trust systems where only those who need access can obtain the information. Only print personal data/business sensitive data when necessary and store or destroy the information in a secure manner.

Employees are expressly prohibited from:

- Introducing any software that attempts to compromise the security of the network and the hardware infrastructure, e.g. password detecting software.
- Seeking to gain access to restricted areas of the Trust’s network.
- Knowingly seeking to access data which they know or ought to know to be confidential unless authorised to do so.
- Introducing any form of computer viruses.
- Carrying out other hacking activities.
- Committing the Trust to any form of contract through the internet, other than ordering of goods authorised within the Trust’s supplies procedures.

For employee information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material, i.e. hacking
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

3.13. Working Remotely

This procedure applies to an employee’s use of Trust devices and to an employee’s own computer equipment/mobile devices used for Trust’s business when working away from Trust’s premises (working remotely). When working remotely, an employee must follow the requirements.

3.13.1. Working Remotely Using Trust-Supplied Equipment

- Ensure their work cannot be overlooked by any other person or by CCTV. Use a screen protector to prevent shoulder surfing.
- Personal data/business sensitive information may only be accessed using a Trust device
- Take reasonable precautions to safeguard the security of Trust IT equipment.
- Never leave equipment unattended anywhere and lock your workstation when away from it.
- Loss or theft of any IT equipment including , tablets and phones should be reported immediately to the IT Service desk (01482 477877) available 24/7. The incident must also be reported to the police and line manager as soon as possible. This incident should also be logged on Datix.
- Never allow anyone else such as family members to access your devices for personal use such as internet browsing.
- Ensure that any work they do remotely is saved on the Trust’s system or transferred to the Trust’s system as soon as reasonably practicable.
- All Trust desktops and laptops are equipped with VPN connectivity and must be used to access live Trust data.

3.13.2. Working Remotely Using Not-Trust Equipment

- Non-Trust devices may only be used to access NHSmail through the NHSmail Outlook web application.
- Personal/business sensitive information must never be stored on a non-Trust device.
- Do not download attachments on non-Trust equipment. Only use the “Open in browser” option to view attachments.
- Staff must not save passwords in browsers on non-Trust equipment. If you are using publicly available equipment such as an internet café or hotel PC, ensure you clear all browsing history before closing internet explorer.
- Ensure their work cannot be overlooked by any other person or by CCTV. Use a screen protector to prevent shoulder surfing.
- Apply an appropriate level of security to any personal data that comes into their knowledge, possession or control through their employment with the Trust so that the personal data is protected from theft, loss, destruction or damage and unauthorised access and use.
- Ensure that any work they do on non-Trust devices is saved on the Trust’s system or transferred to the Trust’s system as soon as reasonably practicable.

4. EQUALITY AND DIVERSITY

An Equality and Diversity Impact Assessment has been carried out on this document using the Trust-approved EIA.

5. IMPLEMENTATION

This procedure will be disseminated by the method described in the Document Control Policy.

Line managers must notify new starters of the procedure. This will be prompted on the Induction Checklist.

6. MONITORING AND AUDIT

All breaches and suspected breaches of this procedure must be reported, via your line manager, using Datix. The Risk Management Team will inform the Head of IT Services and Information Governance Team of any breaches.

The monitoring of electronic communication follows strict guidelines which are identified in Monitoring Electronic Communications Procedure detailed in Appendix 4. All monitoring of electronic communications controlled by the Trust must follow this procedure and be authorised by the Information Governance Group.

The Trust will respect an employee's privacy and autonomy in business communications. However, in certain circumstances it may sometimes be necessary to access and record an employee's business communications for the Trust's business purposes which include the following:

- Providing evidence of business transactions.
- Making sure the Trust's business procedures, policies and contract are adhered to.
- Complying with any legal obligations, including Subject Access Requests.
- Training and monitoring standards of service.
- Preventing or detecting unauthorised use of the Trust's communication systems or criminal activities.
- Preventing, detecting or investigating NHS Fraud or Corruption.
- Maintaining the effective operation of the Trust's communication systems.
- Business continuity.

6.1. Emails

NHSmail email data may be accessed for investigation purposes. Requests must be authorised by the HR director or SIRO and forwarded to the Head of IT Services following the usual investigative process. Depending on the information required, the request may need to be authorised by the Trust's Chief Executive or HR Director in writing to the NHSmail programme head. Please see NHSmail: Access to Data Procedure for further information.

NHSmail data may be accessed for subject access requests. A request will be made to the mailbox owner to search for the required information. Support with the searches can be provided by the IG Team to the mailbox owner.

The IG Team can obtain a copy of the mailbox, if necessary, e.g. if a staff member is not available to conduct the searches. This will be with authorisation from the Caldicott Guardian, SIRO or Data Protection Officer. Only emails relating to the search criteria will be accessed and only personal data related to the data subject will be released. If the IG Team obtain a copy of the mailbox, an email notification will be sent automatically to the mailbox owner by NHSmail.

The Trust will not normally access emails marked "Personal" or "Confidential" unless it has a pressing business need to do so, e.g. to prevent or detect criminal activity involving emails or where a worker is suspected of using email to harass other employees. This must be sufficient to justify the degree of intrusion involved and there must be no reasonable, less intrusive alternative.

Emails sent without the correct identifier (e.g. "Personal" or "Confidential") in the subject line may be accessed by the Trust and such communications recorded as if they were business communications since the Trust will have no way of knowing that they were intended to be personal.

6.2. Mobile Phone

During absences, line managers may have access to their member of staff work issued mobile phone if required for business continuity purposes. Managers must avoid opening any messages that are clearly personal. For transparency, managers will advise staff of this at the point the mobile phone is collected/handed in. For telephone calls, managers/staff can make alternative arrangements, such as a voice mail messages explaining the absence and providing an alternative number.

6.3. Internet

The organisation trusts its employees to use the internet sensibly. Employees need to remember at all times that when visiting an internet site the unique address for that computer (IP address) can be logged by the site that has been visited so the Trust can be identified. Therefore any internet activity that is carried out may affect the Trust.

To protect the integrity, security and efficiency of the Trust's network, internet activity may be recorded. This details the user, web site address and the date and time the website was visited.

This monitoring has been subject to an impact assessment, as detailed in the procedure in Appendix 4 and has been approved by the Information Governance Group.

7. REFERENCES/EVIDENCE/GLOSSARY/DEFINITIONS

7.1. References

NHSmail: Sharing Sensitive Information Guide by Email - A guide for Health and Social Care Email Users
NHSmail: Encryption Guide for NHSmail
NHSmail: Access to Data Procedure
Email and text message communications - NHS Transformation Directorate (england.nhs.uk)
Video conferencing with colleagues - NHS Transformation Directorate (england.nhs.uk)

7.2. Glossary of Terms/Definitions

See Appendix 1.

8. RELEVANT POLICIES/PROCEDURES/PROTOCOLS/GUIDELINES

Disciplinary Policy and Procedure HR-006
Freedom of Information Policy P017
Bullying and Harassment Policy HR-002
Information Security and Risk Policy P096
Confidentiality Code of Conduct Policy N-061
NHSmail Acceptable Use Policy
NHSmail Access to Data Policy
Upstream - IT guidance for Upstream video consultation.pdf (humber.nhs.uk)
Patient Video Consultations SOP20-038.pdf (humber.nhs.uk)

Appendix 1: Glossary of Terms

Anonymised Information	Information that does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.
Business sensitive	Information which, if compromised through alteration, corruption, loss, misuse or unauthorised disclosure, is likely to adversely affect the Trust or other Third party (See Code of Conduct for employees in respect of confidentiality and information security for further information).
Defamation	A published (spoken or written) statement or series of statements that affects the reputation of a person (a person can be a human being or an organisation) and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true then it is considered slanderous or libellous and the person towards whom it is made has redress in law. Liability for the tort of defamation applies to electronic communication just as it does to more traditional forms of publishing (i.e. carries the same legal implication as writing a letter).
Encryption	Prevents any non-authorised party from reading or changing data. The level of protection provided by encryption is determined by an encryption algorithm.
Harassment	A conduct which is unwanted by the recipient or affects the dignity of any individual or groups at work. It normally affects anyone who is perceived as different or is in a minority or in a less powerful position.
Junk mail	An unwanted or unsolicited email advertising a product or service.
Personal data	Data that identifies and relates to an individual
Pornography	The Trust defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting.
Spam	An inappropriate attempt to send junk mail to a large number of people who did not ask for it. Mass junk mail.
Trust network	The secure drive for storing information that is backed up on a daily basis e.g. V Drive, O Drive

Appendix 2: Consent Form for System Generated Electronic Messages

Service address

Dear Patient,

As part of our continuous process to improve service to our patients, we use an electronic messaging service. This means we will be able to send text messages to a mobile phone of your choice to remind you of appointments, send notifications that test results have been received and other messages regarding improvements and services. Such messages and information may also be sent via email.

We may need to update our records to include an up to date mobile telephone number and email address and also have consent from you in order for us to send messages to your mobile phone or email address.

If you would like to receive information in this way, please complete the information below.

Name	
NHS Number (if known)	
Address	
DOB	
Home Telephone Number	
Mobile Telephone Number	
Email address	

I do/do not (delete as appropriate) give my consent for [Service Name] to send text messages as described above to my mobile telephone or my email address. I understand that I can withdraw my consent at any time by speaking to the team providing care. I understand I am responsible for providing an up-to-date email address/mobile phone number.

Signed……….…

Dated…….

<u>Office Use Only</u>

Mobile Phone Number/email address recorded	
Consent Recorded	

Appendix 3: Consent Form for Communicating with Individual Patients via Text/Email

When you are receiving a service from us, we want to keep in contact with you. We will do this in the way that is easiest or most convenient for you. We understand that people use email and mobile phone texts, and we also understand that you may want to let someone else receive or send messages for you. This could be someone who is looking after you or someone who you have chosen to help you.

If you tell us that you would like to use email or mobile phone texts in this way, we need to agree about how we do it and this is explained below:

1. We will use email or text because you have told us this is how you want to keep in contact with us.

2. When sending messages outside of the NHS, there might be a risk of someone seeing the message who shouldn’t. To make it safer you should:

   - Try not to use a public or work computer.
   - Let us know right away if you change your email address or mobile phone number.
   - Do your best to keep the messages safe and confidential, for example do not leave your computer switched on when you are not there and don’t tell somebody else your password.
   - Have a PIN code on your mobile phone and keep it secret.

3. Depending on the service you are receiving, it may be possible for you to send emails or texts to a Trust email address or mobile phone number. In such cases, you should:

   - Only send messages containing non-sensitive and non-urgent issues.
   - Include your full name in the main part of an email so that we can correctly identify you.
   - Keep personal data sent in text messages to a minimum (your key worker will hold your contact details in an encrypted or pin coded mobile phone).

4. Your emails, text/voice messages to Trust mobile phones will be treated as non-urgent. We cannot say exactly when they will be actioned. If you need to contact us urgently you should telephone us on ………………………………… (Team to specify manned telephone number).

5. We will have to end this agreement if we find out that our systems are at risk from things such as computer viruses that are being sent.

6. When you send us a message, we will make a record of it in your notes.

I accept the above conditions and agree for email/mobile phone texts (delete whichever does not apply) to be used to communicate with me and the Trust.

Email address to be used…………………………………………………………………………….

☐ I would like emails to be sent securely using the NHS encryption service. I understand I will need to register for this service electronically (Tick if applicable)

Mobile phone number to be used……………………………………………………………………

Name of carer or advocate who I nominate for messages ………………………………………
(If applicable)

If you give consent but would like to restrict the information that is shared using email/mobile phone texts (e.g. information about appointments only) please provide details below.

………………………………………………………………………………………………………

………………………………………………………………………………………………………

NAME:…………………..…..…………SIGNED………………….........DATE…..…………………

(Service user)

I accept the above conditions when communicating on behalf of the service user using the above email address.

NAME: ……………………………..……SIGNED…………………………DATE….…………………
(Advocate/Carer)

Service user's copy ☐ Health Records Copy

Appendix 4: Procedure for Monitoring Electronic Communications

1. INTRODUCTION

The aim of this procedure is to detail how the Trust will monitor electronic communications to ensure that the requirements of the Data Protection Act 2018, UK General Data Protection Regulation, Regulation of Investigatory Power Act 2000 and Lawful Business Practice Regulations are met.

2. LEGAL REQUIREMENTS

To ensure compliance with legislation, all monitoring must comply with the following:

- Those who have access to personal information obtained through monitoring will be kept to minimum.
- Personal information collected through monitoring will not be used for any other purpose unless it is clearly in the individual's interests to do so, or it reveals an activity that the Trust could not reasonably be expected to ignore.
- Employees will be informed about the monitoring that takes place and why (unless covert monitoring is justified), the monitoring information that is held and how long this information is kept for.
- Employees will be able to explain or challenge the results of any monitoring through the Trust disciplinary or grievance procedure.
- Employees will have the right of access to information about them kept for, or obtained through, monitoring.
- All monitoring involving the interception of communications will be checked for compliance against the Regulation of Investigatory Power Act 2000 and the Lawful Business Practice Regulations.

3. IMPLEMENTATION

To ensure that the above requirements are met, anyone who is considering monitoring electronic communications must complete an Impact Assessment Form. The form will be submitted to the Information Governance Group for authorisation.

Authorisation to monitor using a particular piece of equipment only needs to be sought once. Authorisation is not required each time the equipment is used. However, a new form should be completed if there are significant changes to the monitoring. The form should be submitted to the Information Governance Group for approval.

The Electronic Communications and Internet Acceptable Use Procedure will be reviewed in light of any further monitoring of staff and will be publicised through the intranet and Team Talk.

4. FURTHER INFORMATION

For advice regarding the completion of the form, please contact the Information Governance Team, Tel. 01482 477856.

The forms below are to be used to make an evaluation of the risk faced by the Trust and to assess whether the carrying out of monitoring electronic communications will reduce or eradicate those risks.

IMPACT ASSESSMENT – MONITORING ELECTRONIC COMMUNICATIONS

1	**Type of electronic communication being monitored**	
2	**Purpose** **Please detail the purpose behind the monitoring.**	
3	**Benefits** **Please detail the benefits the monitoring is likely to deliver**	
4	**Adverse impact** Please answer the following questions to determine whether there will be any adverse impact as a result of the monitoring.	
5	**Will there be any intrusion into the private lives of workers and others, or interference with their private emails, telephone calls or other correspondence?**	Yes □ No □ If “yes” please provide details below
6	**Are workers and others aware that the monitoring is taking place?**	Yes □ No □ If “yes” please provide details below
7	**Are workers and others in a position to act to limit any intrusion or other adverse impact on themselves?**	Yes □ No □ If “yes” please provide details below
8	**Will the monitoring mean that information that is confidential, private or otherwise sensitive will be seen by those who do not have a business need to know, e.g. IT workers involved in monitoring email content?**	Yes □ No □ If “yes” please provide details below
9	**Will there be any impact on the relationship of mutual trust and confidence that should exist between workers and their employer?**	Yes □ No □ If “yes” please provide details below
10	**Will there be any impact on other legitimate relationships, e.g. between trades union members and their representatives?**	Yes □ No □ If “yes” please provide details below
11	**Will there be any impact on individuals with professional obligations of confidentiality or secrecy, e.g. solicitors or doctors?**	Yes □ No □ If “yes” please provide details below
12	**Will the monitoring will be oppressive or demeaning?**	Yes □ No □ If “yes” please provide details below
13	**Can established or new methods of supervision, effective training and/or clear communication from managers, rather**	Yes □ No □ If “yes” please provide details below

	than electronic or other systemic monitoring, deliver acceptable results?	
14	**Can the investigation of specific incidents or problems be relied on rather than continuous monitoring?**	Yes □ No □ If “yes” please provide details below
15	**Can monitoring be limited to workers about whom complaints have been received, or about whom there are other grounds to suspect of wrong-doing?**	Yes □ No □ If “yes” please provide details below
16	**Can monitoring be targeted at areas of highest risk, e.g. can it be directed at a few individuals whose jobs mean they pose a particular risk to the business rather than at everyone?**	Yes □ No □ If “yes” please provide details below
17	**Can monitoring be automated? If so, will it be less intrusive, e.g. does it mean that private information will be ‘seen’ only by a machine rather than by other workers?**	Yes □ No □ If “yes” please provide details below
18	**Can spot-checks or audit be undertaken instead of using continuous monitoring? Remember though that continuous automated monitoring could be less intrusive than spot-check or audit that involves human intervention**	Yes □ No □ If “yes” please provide details below
	Obligations Please answer the following questions to ensure that any legal obligations are met.	
19	**What information will be collected about individuals as a result of the monitoring?**	
20	**Who will have access to the personal information obtained through monitoring?**	
21	**Will the proposed monitoring allow employees to readily have access to information collected about them?**	Yes □ No □ If the answer is “no” this must be built into the system.
22	**How long will the information be retained?**	
23	**How will the information about workers collected through monitoring be kept securely?**	
24	**Does the monitoring involving the interception of a communications?**	Yes □ No □ If “yes” please answer the below question.

25	**Does the monitoring comply with the Regulation of Investigatory Power Act 2000 and the Lawful Business Practice Regulations?**	Yes □ No □ Please provide details below
26	Form completed by: - (Include details of consultation)	
27	Authorisation The monitoring of electronic justifications is/ is not (please delete) justified in these circumstances. Information Governance Group Date of Meeting	

Appendix 5: Electronic Communications and Internet Acceptable Use Procedure Summary

✓	Only send personal data by email using one of the approved methods and following the additional security measures.	✗	Do not send personal data to a non-secure address without using the NHSmail encryption service.
✓	Make sure you have the correct recipient. If you are unsure, send a test email or ask the recipient to email you before sending any personal data.	✗	Do Not create, access, download or email any inappropriate or offensive material.
✓	Mark emails appropriately in the subject line, e.g. "personal", "confidential", "business sensitive".	✗	Do not use the internet for personal use or send personal emails during working hours.
✓	Edit your entry on the NHSmail directory to provide information such as location, address, telephone number, job title and department.	✗	Do not open attachments containing confidential or business sensitive information on computers that do not belong to the Trust, even via the secure NHSmail logon.
✓	Use the "Automatic Replies" function when you are away from the office for more than 24 hours.	✗	Do not stream media over the internet
✓	Take care with the content of emails – they can be legally binding and are subject to the Freedom of Information Act. Follow the etiquette guidelines.	✗	Do not forward emails, e.g. chain letters, junk mail, jokes and emails containing dynamic information (video clips, macro, software etc.)
✓	Keep your inbox/sent items to a minimum, saving any emails that need to be kept in the correct Trust repository e.g. Trust network or clinic system.	✗	Do not use the internet/email for personal business purposes, e.g. renting out your holiday cottage.
✓	Lock your PC when you leave your work area.	✗	Do not automatically forward emails to addresses outside the global address book.
✓	Delete emails from unknown sources without opening them.	✗	Do not share your password.
✓	Contact the IT Service Desk if you suspect a virus may be attached to a file download or an email.	✗	Do not allow other people to view Trust information when working remotely.

Remember – internet use may be subject to monitoring – see Section 8 of the procedure

Appendix 6: Equality Impact Assessment

Equality Impact Assessment (EIA) Toolkit

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. Document or Process or Service Name: Electronic Communications and Internet Acceptable Use Procedure

2. EIA Reviewer (name, job title, base and contact details): Karen Robinson, Information Governance Officer, Mary Seacole Building, 01482 477856.

3. Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other? Procedure

Main Aims of the Document, Process or Service The Information Governance Policy describes the Trust's information governance management and accountability structures, governance processes, documented policies and procedures, staff training and resources.
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group 1. Age 2. Disability 3. Sex 4. Marriage/Civil Partnership 5. Pregnancy/Maternity 6. Race 7. Religion/Belief 8. Sexual Orientation 9. Gender re-assignment	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed? Equality Impact Score Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	How have you arrived at the equality impact score? a) who have you consulted with b) what have they said c) what information or data have you used d) where are the gaps in your analysis e) how will your document/process or service promote equality and diversity good practice

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Age	Including specific ages and age groups: Older people Young people Children Early years	**Low**	The requirements of this policy apply only to adults working for or on behalf of the Trust. The IG issues log and quarterly reports to the IG Committee are scrutinised and any issues arising which relate specifically to equality impact would be identified through that process.
Disability	Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities: Sensory Physical Learning Mental health (including cancer, HIV, multiple sclerosis)	**Low**	As above
Sex	Men/Male Women/Female	**Low**	As above
Marriage/Civil Partnership		**Low**	As above
Pregnancy/ Maternity		**Low**	As above

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Race	Colour Nationality Ethnic/national origins	**Low**	As above
Religion or Belief	All religions Including lack of religion or belief and where belief includes any religious or philosophical belief	**Low**	As above
Sexual Orientation	Lesbian Gay men Bisexual	**Low**	As above
Gender reassignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	**Low**	As above

Summary

Please describe the main points/actions arising from your assessment that supports your decision above All the requirements apply equally to all staff working across the Trust. There is no evidence of potentially negative effect on groups in the categories above.	
EIA Reviewer – Karen Robinson	
Date completed: 15 May 2024	Signature: K Robinson