One + all | we care

Royal Cornwall Hospitals NHS Trust

Cornwall Partnership NHS Foundation Trust

Kernow Clinical Commissioning Group

Cornwall and Isle of Scilly NHS Community E-mail Policy

V3.1

March 2020

Table of Contents

1. Introduction

1.1. Email is an established method for day to day internal and external communication by NHS organisations. It can be of great benefit to the NHS when used appropriately. Its use, however, also exposes the NHS organisation and individual users to risks. This includes the risk of legal action due to breaches of, for example, data protection and confidentiality requirements, threats to IT and information security and ineffective communication. If these risks materialise either the NHS organisation or the individual employee are at risk of prosecution, which would have a negative impact on the reputation of the NHS organisation and could lead to financial penalty following legal action. Care must therefore always be taken to ensure that the email is to the intended recipient and that the content is appropriate to be sent as an email.

1.2. Email is not always the best way to communicate information as email messages can often be misunderstood. The pure volume of email messages can also be prohibitive to effective communication as a result of email overload. Emails should be treated with the same level of attention that is given to drafting and managing formal letters and memos. As well as taking care over how email messages are written, emails should be managed appropriately after they have been sent or received.

1.3. This policy clearly sets the expectations of the Cornwall and Isles of Scilly Health community (consisting of the Royal Cornwall Hospitals Trust, Cornwall Partnership Foundation NHS Trust, and NHS Kernow Clinical Commissioning Group), hereafter known as the Trust, staff members, managers and Cornwall IT Services (CITS) in the use and management of the email system, including accessing personal web-based email accounts on Trust equipment.

1.4. Staff should ensure that they are familiar with the content of this policy and use it as a point of reference when dealing with email messages.

1.5. This version supersedes any previous versions of this document.

1.6. **Data Protection Act 2018 (General Data Protection Regulation – GDPR) Legislation**

The Trust has a duty under the DPA18 to ensure that there is a valid legal basis to process personal and sensitive data. The legal basis for processing must be identified and documented before the processing begins. In many cases we may need consent; this must be explicit, informed and documented. We can't rely on Opt out, it must be Opt in.

DPA18 is applicable to all staff; this includes those working as contractors and providers of services.

For more information about your obligations under the DPA18 please see the 'information use framework policy', or contact the Information Governance Team rch-tr.infogov@nhs.net

2. Purpose of this Policy/Procedure

2.1. The purpose of the policy is to aid the effective and appropriate use of email on Trust systems and to reduce the risk of adverse events by:

- setting out the rules governing the sending, receiving, and storing of email
- establishing Trust and user rights and responsibilities for the use of the email system
- promoting awareness of and adherence to current legal requirements and NHS information governance standards.

2.2. This policy has been written to meet the requirements of:

- the Data Protection Act 2018 (GDPR)
- the Human Rights Act 1998
- common law duty of confidentiality
- the Computer Misuse Act 1990
- the Environmental Information Regulations 2004
- NHS Code of Practice on Confidentiality
- Caldicott Principles
- NHS Care Record Guarantee
- NHSmail Access Policy
- NHSmail Acceptable Use Policy
- NHSmail Access to Data Policy
- NHSmail Information Management Policy
- NHSmail Data Retention Policy

3. Scope

This policy applies to all staff members and their use of:

- NHSmail for business and personal use on Trust and non-Trust premises including from home, internet cafes and via mobile devices.
- personal web-based email accounts accessed from Trust equipment.

4. Definitions / Glossary

4.1. Cornwall NHS managed network – NHS National Network (N3), the Health and Social Care Network (HSCN) and local networks and IT systems connecting the Trusts and partner organisations in Cornwall for the delivery of NHS services managed by Cornwall IT Services (CITS).

4.2. CITS Service Desk – The IT helpdesk which provides IT support and administration functions as well as a central point to report IT related incidents.

4.3. Personal web-based email accounts - Examples include Gmail, Hotmail, Yahoo!, AOL and other email services provided by Internet Service Providers such as BT, Orange or TalkTalk.

4.4. ESR Electronic Staff Record. The human resources and payroll database system currently used by the NHS organisations in Cornwall to manage the payroll for the staff members.

4.5. LOA - Local Organisation Administrator. A staff member appointed by the Trust to look after and manage the NHSmail accounts in the Trust, to receive and digest regular reports on the Trust's NHSmail accounts and to distribute summarised information from these reports to all relevant parties.

5. Ownership and Responsibilities

5.1. The Trust provides access to NHSmail to staff members primarily for use in their:

- work duties
- work related educational purposes
- work related research purposes.

5.2. The Trust allows personal use of NHSmail provided this does not interfere with the performance of your duties, those of other staff or contractors or the business of the Trust in general. Personal access to NHSmail can be limited or denied by your manager. Staff members must act in accordance with Trust Policies and their manager's locally imposed restrictions.

5.3. No staff member has the right to an NHSmail account. On this basis the inappropriate use or abuse of email may result in access being withdrawn or amended.

5.4. The Trust reserves the right to remove or amend access to NHSmail at any time in order to protect and preserve the integrity and confidentiality of the system.

5.5. Role of the Managers

5.5.1. Line managers are responsible for:

- ensuring that the staff members they manage are aware of this policy and their individual responsibility for complying with it
- ensuring their staff members are equipped to fulfil those responsibilities; this will include meeting specific and generic training needs through personal development plans

5.5.2. Managers have specific responsibilities at each stage of a staff member's employment:

- starters – managers should ensure ALL new staff members have read and understood the Confidentiality: NHS Code of Practice prior to giving a staff member access to NHSmail - failure to comply by a staff member

may lead to disciplinary action

- movers/leavers – managers should work with a staff member that leaves or changes role to transfer any Trust information (including any emails, documents and the contents of their archives) stored within their NHSmail account to either an appropriate person or shared work area, for purposes of business continuity; this will include ensuring that all patient and organisationally sensitive information is deleted from the account and ensuring that the remaining contents of the NHSmail account (emails, contacts, documents and the remaining contents of their archive) is made available only for future use with another NHS employer
- senior managers should ensure that managers within their service are aware of their responsibilities in relation to informing staff about acceptable standards of information governance in relation to their staff members' use of NHSmail.

5.6. Role of Individual Staff

All staff members with access to NHSmail are responsible for:

- the correct daily usage of their NHSmail account in line with their job role and associated business functions, ensuring that the account is never used by others and their passwords are never compromised
- changing their NHSmail password immediately if they believe that their password has been compromised
- making themselves aware of the policy and procedure documents relating to access to NHSmail and acceptable use
- raising any queries about the implementation of NHSmail with their line manager or the CITS IT Service Desk
- notifying the CITS IT Service Desk of any changes to personal information or access to NHSmail
- alerting their line manager of any non-compliance with the Email Policy
- reporting information incidents and near misses, including breaches of this policy and incidents where their NHSmail account password might have been compromised, in line with the Procedure for Reporting IM&T Security Incidents.

5.7. Role of Cornwall IT Services

- Cornwall IT Services are responsible for:
- providing access to NHSmail and ensuring that such access is compliant with the Health and Social Care Information Centre (NHS Digital) Data Security and Protection Toolkit (formerly the Information Governance Toolkit) standards (while it is recognised that compliance can only be achieved at an individual's level, the proper management of NHSmail is an important control in ensuring members of staff comply with NHS, local and national standards, e.g. securing information in transit)
- to appoint an LOA for the Trust to look after and manage the NHSmail

accounts in the Trust, to receive and digest regular reports on the Trust's NHSmail accounts and to distribute summarised information from these reports to all relevant parties

- to administer NHSmail (i.e. create and suspend accounts) in accordance with local procedures and to provide support in the use of NHSmail
- to provide guidance on NHSmail use to ensure compliance with NHS standards, Trust policies and UK law
- to provide information from an individual's NHSmail account when requested to support an official investigation
- to assist with providing access in the absence of a staff member for business continuity purposes and to ensure that access is provided in line with this policy.

6. Standards and Practice

6.1. This policy is based on current UK law, NHS information governance standards, and accepted standards of good practice. Staff members' duty to handle Trust and person identifiable information appropriately arises out of common law, legal obligations, staff employment contracts, and professional obligations.

6.2. Any breaches of this policy may result in your employment or your association with the Trust being terminated. It may also bring into question your professional registration and may result in disciplinary, civil, or criminal proceedings.

6.3. If there is anything that isn't clear or which you do not understand in this policy you must contact your line manager, in the first instance, or the Head of Information Governance for further information.

6.4. Please note that the procedures and policies outlined in this policy and any related policy may be changed at any time. You will be alerted to this via established Trust communication routes.

6.5. New Starters

The manager will submit a request for an NHSmail account via the CITS OnForm system. The CITS Service Desk will confirm the validity of the request before the NHSmail account is created and access to the account is provided to the new staff member.

6.6. Movers and Personal Information Changes

6.6.1. When a staff member changes roles within the Trust or changes their personal information they should notify the CITS Service Desk at the earliest opportunity. Upon receipt of the notification and validation of the request the CITS Service Desk will amend the staff member's NHSmail account details based on the information provided.

6.6.2. The personal information that is typically recorded on the NHSmail systems and that can be changed is:

- title
- first, middle and last name
- job title
- base
- work telephone number.

6.7. Changes to Employment Status

6.7.1. When a staff member has their employment status changed to an inactive status that may be the result of an official investigation, the manager should notify the CITS Service Desk to ensure that any access to NHSmail is disabled if appropriate in a timely fashion and maintained consistently with the information available to the manager.

6.7.2. Upon receipt of the notification the CITS Service Desk will suspend the NHSmail account.

6.7.3. If access to specific Trust emails or proxy access to the NHSmail account is required whilst the user account is suspended the manager should request either access in the absence of a staff member or access in the event of an investigation depending on their requirements.

6.7.4. The NHSmail account will have appropriate comments applied to it by the CITS Service Desk to ensure that the account is not made active without appropriate authority.

6.7.5. The inactive status' that should be notified to the CITS Service Desk are:

- maternity
- long-term sickness
- suspend assignment
- suspend with pay
- suspend no pay
- suspend contingent assignment.

6.7.6. When the employment status is changed to an 'active' status the manager should notify the CITS Service Desk who will make the NHSmail account active and remove any associated comments.

6.8. Secondments

6.8.1. Staff going on secondment within the Trust should be treated as a mover.

6.8.2. Staff going on secondment to another NHS organisation should be treated as a leaver and joined to the new organisation within 30 days.

6.9. Temporary Staff

Temporary staff may need access to NHSmail as part of their role. The following points should be considered:

- temporary staff working as part of a team may not need an NHSmail account to fulfil the role
- some temporary staff could already have an NHSmail account
- temporary staff who are provided with access to NHSmail may not have sufficient training in the use of NHSmail.

6.10. Long-Term Access Assignments

6.10.1. When a temporary staff member is placed on a long-term assignment, typically covering long-term sickness, for example, the manager should notify the CITS Service Desk with details of the assignment.

6.10.2. The temporary staff member will be provided with access to NHSmail or their personal information on NHSmail will be updated on NHSmail to reflect their current assignment.

6.10.3. At the end of the assignment the manager should notify the CITS Service Desk who will update the temporary staff member's personal information to reflect the end of the assignment and will remove any access to NHSmail if appropriate.

6.11. Staff not Directly Employed by the Trust

6.11.1. The Trust acknowledges that there are some instances where staff members are not directly employed by the Trust.

6.11.2. Staff members not directly employed by the Trust will include, but are not limited to, the following groups:

- trainees
- contractors
- students
- researchers
- trainers
- consultants.

6.11.3. The manager of a staff member not directly employed by the Trust requiring an NHSmail account should submit a request via the CITS OnForm system.

6.11.4. Staff not directly employed by the Trust should notify the CITS Service Desk of changes to personal information along with approval from the manager.

6.11.5. The manager is responsible for notifying the CITS Service Desk when staff members not directly employed by the Trust leave or when their contractual status within the Trust becomes inactive.

6.12. Generic Accounts

6.12.1. The use of generic accounts should be avoided as far as practically possible due to the increased IT security risks they pose.

6.12.2. Where there is a genuine need for a generic NHSmail account this should be requested by the staff member who should submit a Generic Account Request Form to the manager. At this point the request is verified prior to the request being forwarded to the CITS Service Desk for the NHSmail account to be created.

6.12.3. Generic (Resource) Accounts
A generic (resource) account is a shared account that is not typically associated with one user. It is usually accessed by multiple staff members from the same department or project. For example, for managing access to a specific resource e.g. a meeting room. All staff members who have access to the generic account can send emails 'on behalf' of the account.

6.12.4. Generic accounts must be set up by the CITS Service Desk who will also set the access permissions. Generic account names will always be prefixed by the owning organisation's "short code", e.g. rch-tr.accountname@nhs.net.

6.12.5. Generic accounts are specifically linked to the Trust and cannot be migrated to another organisation the same as a person account specifically assigned to an individual staff member.

6.12.6. Generic accounts are not accessed with a username and password but via a staff member's own NHSmail account when they are logged in.

6.12.7. Generic (Ghost) NHSmail Accounts
A generic (ghost) NHSmail account, or generically named account is a person NHSmail account which has been named to reflect the purpose for which it was created, e.g. trelawney.reception@nhs.net. This type of account should be used when there is a specific requirement to directly and routinely access and monitor the account, e.g. to retrieve specific emails.

6.12.8. If the account is to be monitored directly and routinely by multiple staff members rather than by a system, sharing permissions will need to be set up. The manager will need to act as the owner and would provide permission for other staff members to access the account.

6.13. Dual Employment

6.13.1. Where a staff member has dual employment with two, or more, NHS organisations the substantive or earliest employer will determine which

organisation their named NHSmail account will be associated with. Multiple NHSmail accounts for the same staff member will not be permitted.

6.13.2. It is the dual-employed staff member's responsibility to manage the sending and receiving of emails to and from their NHSmail account to ensure that emails relating to separate NHS employers are handled appropriately and that any information contained within emails is separated accordingly.

6.13.3. To enable the recipient to easily identify which organisation an email is being sent from in the case of dual employment it is suggested that an alternative email signature is used, clearly identifying the associated role and employer.

6.14. Account Maintenance

6.14.1. Password Resets

6.14.1.1. Staff members who have forgotten their NHSmail password should follow the link on http://www.nhs.net for Reset Forgotten Password to complete a self-service password reset.

6.14.1.2. Staff members who suspect that their NHSmail account may be compromised or suspect that the password is known by another or who have been locked out of NHSmail should report the problem to the CITS Service Desk as soon as is practical.

6.14.1.3. The staff member must confirm their identity before the password is reset.

6.14.2. Inactive Accounts

6.14.2.1. NHSmail accounts will be regularly monitored to identify inactive accounts. Any NHSmail person accounts, including generic ghost accounts, that are found to be inactive for longer than 90 days will be handled in line with the NHSmail Information Management Policy.

6.14.2.2. Any NHSmail generic (resource) accounts that are found to be inactive for longer than six months will be handled in the same way.

6.14.2.3. Suspended accounts will be automatically removed eighteen months after the date of the suspension if no further changes have been made to the employment status.

6.14.2.4. Pre-provisioned accounts that are not activated by the staff member within three months of creation will be deleted automatically.

6.14.3. Compromised Accounts

6.14.3.1. Where it is identified that an NHSmail password has been compromised or known by another person, staff member or otherwise, the

CITS Service Desk will suspend the account and report this as an incident to the IT Security Management Team.

6.14.3.2. The severity of the incident will determine whether access to the compromised account is reinstated, to whom and when.

6.14.3.3. A similar process will be followed where unauthorised access is identified, particularly in relation to dual employment accounts.

6.14.4. Leavers

6.14.4.1. The CITS Service Desk will receive regular scheduled ESR reports to identify staff members directly employed by the Trust that have left.

6.14.4.2. This information will be used to deactivate the relevant NHSmail account for a period of 30 days.

6.14.4.3. After 30 days, if the NHSmail account has not been 'joined' to a new NHS organisation then the account will be deleted.

6.15. Managing emails

6.15.1. NHSmail is a communication and collaboration tool and not a records management system. Where the content of an email may be needed in the future it is the responsibility of the staff member to ensure it is stored appropriately (archived) within the corporate or clinical records system.

6.15.2. Storage space for emails is limited to a maximum allocation determined by NHSmail. Exceeding the allocated space could result in the corruption and loss of your emails and/or attachments.

6.16. Use of emails

6.16.1. Staff members should use email only when it is appropriate to do so and not as a substitute for verbal communication. Emails should be worded with care because voice inflections cannot be picked up and it can be difficult to interpret the 'tone' of a message.

6.16.2. Email is a formal method of communication and should be treated the same as if writing a letter.

6.16.3. Email messages must not include anything that would offend or embarrass any reader or would embarrass the Trust if it found its way into the public domain.

6.16.4. Write ALL emails on the assumption that they may be read by others, particularly people who do not normally work for the Trust such as temporary staff. Email is easily forwarded on and may be read by unintended recipients.

6.16.5. Limit the number of recipients the email is sent to only as many recipients as is absolutely necessary. All staff members with access to NHSmail have a responsibility to not overload other staff members with irrelevant emails and not to put pressure on recipients by copying in 'people with authority' unnecessarily.

6.16.6. A concise and meaningful title should be put in the subject heading of every email to indicate its content. This will assist the recipient in prioritising the opening of email and aids the retrieval of opened messages.

6.16.7. Staff members should not use email as the only method of communication if an urgent response is required.

6.16.8. Where important information has been sent by email, confirmation of receipt must be obtained either by email or by a follow up telephone call.

6.16.9. Staff members must access NHSmail regularly and respond to messages in a timely manner.

6.16.10. Staff members should indicate when they are not able to read their email (for example, when on annual leave) by using the tools within NHSmail (such as an 'out of office' notification).

6.16.11. Inappropriate use may result in poor communication, impede the function of the Trust's network system, impede the effective functioning of NHSmail, or compromise the security of the system.

6.16.12. Staff members must only use a disclaimer that has been authorised.

6.17. Legal requirements

6.17.1. The use of NHSmail must comply with UK law and adhere to Trust rules, codes of conduct, policies and procedures.

6.17.2. Staff members must not use NHSmail for any purpose that conflicts with their contract of employment.

6.17.3. Email messages have the same legal status as other written documents and must be disclosed in legal proceedings if relevant to the issues. The content of any emails may be disclosed under the Data Protection Act 2018 (General Data Protection Regulations), Freedom of Information Act 2000 and the Environmental Information Regulations 2004. Therefore, the author must ensure the content, style and language used is appropriate, as any data subjects mentioned may legally request access to the emails as a Subject Access Request under the Data Protection Act.

6.17.4. Improper statements may result in the Trust and/or the staff member being liable under law.

6.18. Security

6.18.1. Passwords and login credentials for NHSmail must be kept confidential (no staff member or NHSmail support staff member should ever ask you to divulge your password).

6.18.2. Sharing passwords or login credentials will be considered misconduct. Where necessary, staff members can give proxy access to their NHSmail account. This should normally be read access but may allow full access depending on the relationship.

6.18.3. There is no right for a manager to demand access to a staff member's NHSmail account unless there is a legitimate business continuity requirement, official investigation, request under the Data Protection Act, Freedom of Information Act or the Environmental Information Regulations. that requires such access. In all cases this needs to be provided in accordance with the relevant standards and practice

6.18.4. NHSmail passwords should be changed regularly (at least every 90 days) and should be complex in nature, e.g.:

- minimum length of 8 characters containing upper and lower case, numeric and/or special characters
- should not be easy to guess – never use family members or pet's names, telephone numbers, car make and model or registration number, etc.
- should not be a recognisable word (these are vulnerable to automated 'dictionary' attacks).

6.18.5. If a tablet or smartphone has been set up to access NHSmail a range of security features are automatically applied to it to minimise the risk of data loss.

6.18.6. The security features enabled include:

- an encrypted connection between the mobile device and the NHSmail service
- implementation of a password to access the mobile device
- a limit on the size of email attachments that can be downloaded
- a remote wipe facility allowing the data held on the mobile device to be deleted if it is lost or stolen

6.18.7. The default NHSmail mobile device security policy is described in **Appendix 3** of this document.

6.18.8. Once the policies have been applied to the mobile device they can only be removed by performing a factory reset (format) of the device.

6.18.9. If the policies are not applied correctly to your device, you must inform the CITS Service Desk to ensure that you are not in breach of Trust

policy.

6.18.10. In addition, some mobile devices automatically encrypt the data they contain “at rest”, helping to preventing access should it be lost or stolen. Encryption at rest is automatically enabled on connection to NHSmail on those devices that support this feature.

6.18.11. It is important that sensitive or personal identifiable information isn’t held on any mobile device that does not have built-in encryption at rest capability or one where encryption at rest cannot be remotely enabled. It is a mandatory Department of Health requirement that such data should only be carried on an encrypted device.

6.18.12. A list of compatible mobile devices is listed in Appendix 4 of this document. If your mobile device isn’t listed please contact the CITS Service Desk for further guidance before it is used to hold or transmit sensitive or personal identifiable information.

6.18.13. Trust email password security is particularly important as NHSmail is accessible via the internet and therefore your username and password are the only security controls safeguarding the information stored within a staff member’s NHSmail account.

6.18.14. Staff members should logout of NHSmail when they have finished using it and must lock their computer when leaving it, for example, to make a cup of tea, to attend a meeting or to go for lunch.

6.18.15. When accessing NHSmail via a mobile device or via the Internet, it is the staff member’s responsibility to ensure that emails are not viewable or accessible by any other person.

6.18.16. You should only access NHSmail on a non-NHS Windows computer, i.e. a home computer, personally owned laptop or in an Internet café, via the web at www.nhs.net and not via an email programme such as Microsoft Outlook unless you have explicit permission from the Trust to do so.

6.18.17. When you access NHSmail from a non-NHS computer at www.nhs.net you should select the “This is a public or shared computer” login option to prevent any files being unintentionally left on the computer. You should not change this default option unless you have permission to do so from your manager who should seek advice from the Head of Information Governance.

6.18.18. If you do have permission from your manager to download files to a non-NHS computer you should take the following precautions when accessing email attachments: right click on the file, click ‘Save as’ and then save it to a secure location as advised by the Trust.

6.18.19. Care should be taken with any printed emails that contain confidential information. Printed emails containing confidential information must be stored and disposed of securely and in line with the Records

Retention Policy.

6.18.20. Business related emails sent from or received into NHSmail must not be sent to or forwarded onto personal web-based email accounts.

6.18.21. Personal web-based email accounts should not be used to send or receive business related emails.

6.19. Personal use

6.19.1. The personal use of NHSmail is not discouraged provided this does not interfere with the performance of your duties, those of other staff members or the business of the Trust in general. Personal access to NHSmail can be limited or denied by your manager. Staff and contractors must act in accordance with Trust policies and their manager's locally imposed restrictions.

6.19.2. Personal emails should be stored in a folder marked 'personal'.

6.19.3. Special care should be taken when using your NHSmail account to send personal emails as these emails will inherently carry the Trust's signature and therefore may be, incorrectly, assumed to be sent on behalf of the Trust rather than of a non-work and personal nature. This is of particular importance when sending emails to statutory bodies or formal establishments where it would be easy to misinterpret the email as a formal communication from one organisation to another.

6.19.4. Only use your NHSmail account to register with authorised social media sites when you have been approved to be acting on behalf of the Trust. Entering into a forum or a blog and making informal suggestions or giving advice using your NHSmail account could be perceived as formal NHS advice from the Trust. In general, when registering for social media sites (Facebook, Twitter, etc.) staff members should use a personal web-based email address.

6.19.5. When using a personal web-based email account you must **never** attach or send any confidential, personal identifiable or sensitive information nor must you use a personal web-based email account to send or attach such information. To do so would be a breach of NHS standards and the Data Protection Act which might lead to disciplinary action. If you know that another staff member is sending or receiving information in this way it should be reported immediately to the CITS Service Desk or direct to the Head of Information Governance.

6.19.6. To enable the recipient to easily identify your message as a personal message rather than one sent on behalf of your organisation in your official role, the following examples of best practice may help:

- prefix the subject with [Personal]
- add a sentence to the start of the message: "This is a personal email, not sent in my official capacity or on behalf of any official NHS business"
- marking an email as personal does not exempt it from discovery or

being used as supporting evidence in any locally initiated investigations.

6.19.7. Although features in NHSmail do allow you to flag an email as personal it is recommended that you do not use this feature as not all receiving email programs display the message flag.

6.20. Misuse of the system

6.20.1. Staff members must not:

- use their NHSmail account to conduct private or freelance work for the purpose of commercial gain
- create, hold, send or forward emails that contain or could be considered to contain obscene, pornographic, sexually, racially or religiously offensive, or otherwise illegal content (If you receive such a message you should report it to the CITS Service Desk immediately)
- create, hold, send or forward emails that are or could be considered to be defamatory, harassing, intimidating, abusive, bullying or contain any other content which breaches Trust or NHS codes of conduct
- create, hold, send or forward emails that contain statements that are untrue, inaccurate, misleading or offensive about any person or organisation
- apply rules that automatically forward all emails outside of NHSmail
- access and use another staff member's NHSmail account without permission (If it is necessary to access another staff member's account then you should contact the CITS Service Desk for details of the necessary procedure)
- provide delegated access to an NHSmail user from another organisation, family member or a friend unless this has been approved as being for legitimate business use and approved by the Head of Information Governance
- gain delegated access to another NHSmail user's account from another organisation, family member or a friend unless this has been approved as being for legitimate business use and approved by the Head of Information Governance
- send email messages from another staff member's NHSmail account without it being clear the account owner has not been the author of the content - where a nominated member of staff has been given the authorisation to send emails from another NHSmail account, it should be made clear within the email, who the email is actually from, i.e. from <Personal Assistants name> on behalf of <email account name> (Personal Assistants and other nominated staff may send emails from their own NHSmail account on behalf of their manager if instructed to do so)
- send global emails to ALL staff outside of agreed processes for such communications (Contact your manager, who will in turn ensure it is sent via approved routes, e.g. Daily/Weekly Bulletins)

- send or forward any email from their NHSmail account that could be considered spam, contains offensive material or is a ‘chain letter’ sent on by others (u sing an NHSmail address gives the recipient the impression that the content of the email is endorsed by the NHS
- use their NHSmail account for political lobbying
- knowingly introduce to the system, or send an email or attachment, containing malicious software, for example, viruses
- forge or attempt to forge email messages, for example, spoofing.

6.21. Sending attachments

6.21.1. Consider alternative ways of making large work documents available to other staff members such as placing documents in a shared folder or on the Intranet and emailing a link. Alternatively, use file compression, for example, ‘zip’ files, or other methods of file transfer, for example Secure File Transfer Protocol.

6.21.2. Certain file types and extensions that are considered potentially harmful are blocked on NHSmail. These include executable application files, screen savers, certain audio, movie and video files, script files Windows registry files.

6.21.3. Encrypted attachments cannot be scanned for malicious code by NHSmail and may contain virus infected files. It is the responsibility of the staff member to ensure that they are satisfied that the contents of an encrypted attachment are safe before opening it. Where encrypted attachments are sent inbound from outside of NHSmail the recipient will be notified that the attachment could not be scanned for malicious code.

6.21.4. Additional rules apply to compressed (zip) files in terms of size and number of embedded layers within the zip file.

6.22. Confidential, Personal Identifiable or Sensitive information

6.22.1. The most common cause of unauthorised disclosure of confidential, personal identifiable or sensitive information within the NHS is emails sent to the wrong recipient. It is essential, when sending emails with confidential, personal identifiable or sensitive information, that you ensure that the email address is correct. If you are not 100% certain that you know the correct email address you must use the NHSmail Address Book and select the recipient’s email address. If the intended recipient is not in the address book, you must find another way to confirm the email address.

6.22.2. Confidential, personal identifiable or sensitive information, including information about patients, service users and staff members, should not be sent by email, even if it is encrypted, unless it is part of an approved workflow process authorised by a senior manager and with the associated risk assessment signed off by the Head of Information Governance.

6.22.3. Safe haven procedures must be used when routinely sending confidential, personal identifiable or sensitive information by email to external organisations.

6.22.4. Confidential, personal identifiable or sensitive Trust information when accessed from a non-NHS device must be done so in a secure manner. You should not download this type of information to a non-NHS device. (Arrangements for working outside of this policy require prior approval from the manager who should seek advice from the Head of Information Governance).

6.22.5. When sending patient information you should include the phrase 'Patient Information' in the Subject Field; this ensures that the message is clearly identifiable to the authorised recipient.

6.22.6. If you are sending an email containing confidential, personal identifiable or sensitive information outside of the Trust you must first establish if it is legal to do so. Sharing information without consent could be a breach of the Data Protection Act (if in doubt, please contact the Data Protection Officer for advice).

6.22.7. If you are sending confidential, personal identifiable or sensitive information outside of NHSmail you should type [secure] in the subject header (including the square brackets), this will ensure appropriate security measures are applied before it leaves NHSmail. Further advice on when you should encrypt emails can be found in **Appendix 5**. If this is the first time the recipient has received an encrypted email from NHSmail, you should send the following guidance in a separate email that explains the process to retrieve, read and reply to an NHSmail encrypted email: **Accessing Encrypted Emails Guide for Non-NHSmail users.**

6.22.8. There may be occasions when you are sending particularly sensitive information and do not wish to use information that will identify the individual within the body of the text. In these cases it is recommended that you speak to the recipient and agree a secret password/ pseudonym that will identify the person between you.

6.22.9. You must not save confidential, personal identifiable or sensitive information, or any archive files associated with your NHSmail account to a local drive (c:, d:, etc.) on your computer. You must save this information to a network drive on a server (h:, s:, etc.).

6.22.10. You should not include names or dates of birth in the subject header, however it is acceptable to use a pseudonym or initials to help the recipient identify the emails content.

6.23. Access in the Absence of a Staff Member

6.23.1. Staff members should ensure that during periods of planned absence, they have made arrangements for proxy access to their NHSmail account by a colleague to ensure business continuity. If the absence is due to unforeseen events (such as illness), it may be necessary for an employee's line

manager to request access to an staff member's NHSmail account for the purposes of business continuity, an official investigation or a request under the Data Protection Act or the Freedom of Information Act that requires such access.

6.23.2. Staff members should ensure that any personal emails are saved in a separate folder to clearly distinguish them from work based information (e.g. labelled as 'Private', 'Confidential' or 'Personal'), so that in the event that proxy access is granted to the NHSmail account, this information should not be accessed.

6.23.3. In the event that proxy access has been granted as a result of a period of absence or for the purposes of normal collaborative working, only work based information should be accessed based on a specific need basis. Information clearly marked as private must not be accessed. If personal or private information is unintentionally accessed it must not be further disclosed.

6.23.4. Access to another staff member's NHSmail account should have the support from the Trust Medical Director, HR Director and Caldicott Guardian and should only be actioned in line with Trust governance procedures. Access to another staff member's NHSmail account should never be granted unless there is a critical need and it is formally sanctioned as above due to the fact that there may be confidential or personal identifiable data in the NHSmail account which should only be seen by that person.

6.23.5. If the staff member is on long-term leave it is recommended that an out of office message is added to the NHSmail account informing senders to re-send the information to an alternative NHSmail address so information is not lost. This does not require access to the NHSmail account itself.

6.23.6. If it is imperative to gain access to the NHSmail account the relevant account could be accessed by changing the password and retrieving specific emails or data if there is something that is needed urgently. This should be carried out under strict guidance from the above mentioned controllers. The NHSmail account should not be left accessible for anyone to view other than the local administrator who should not retrieve or access any emails or data that are not relevant. The NHSmail account should remain untouched after this. The staff member should be informed that their NHSmail account has been accessed, by whom and for what reason via email so that they can read the email as soon as they return to work.

6.24. Access in the Event of an Investigation

6.24.1. It may become necessary in the course of some official investigations, such as formal HR disciplinary investigations, investigations by or on behalf of the Police, the local Counter Fraud Specialist or the Local Security Management Specialist, to give access outside of the normal line management arrangements to emails or data stored in a staff member's NHSmail account.

6.24.2. Any official investigations will be carried out in accordance with legislation such as the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 2018 and the Human Rights Act 1998.

6.24.3. CITS will only accept initial investigation requests relating to a staff member's NHSmail account from the relevant HR Business Partner, the appointed investigating officer, the Local Counter Fraud Specialist or the Local Security Management Specialist.

6.24.4. Investigation requests must be in writing or email and sent to the CITS Service Desk. The communication must include the explicit permission of the requesting officers as outlined above.

6.24.5. The Trust should ensure that if the information to be returned to the investigation contains or is likely to contain personal identifiable data that this information is handled appropriately, maintaining confidentiality at all times.

6.24.6. In addition to the above, the request must contain the following detail:

- the name of the individual/s and their NHSmail email address
- what information is required, e.g.:
    - the contents of a mailbox at a point in time
    - copies of messages sent and/or received to that mailbox over a specified period
    - actions performed over a period (e.g. number of messages sent/received to or from specified addresses)
    - an audit trail of administrator actions.

6.24.7. It should be noted that requests relating to a staff member's NHSmail account may return all emails pertaining to the request, including details of any emails which the staff member has deleted.

6.24.8. Once a correctly formed request has been received CITS will seek the explicit permission of the requesting organisation's officer:

- Chief Executive or HR Director of the NHS Trust
- the Accountable Officer of the Clinical Commissioning Group (and the associated GP practices)

6.24.9. Upon receipt of the explicit permission from the requesting organisation's officer CITS will send the request to the NHSmail Programme. No service level is associated with investigation requests and all requests will be handled on a 'first come, first served basis'.

6.24.10. Once NHSmail has completed the request the information will be provided via CITS to the requestor in one of the following ways:

- in an NHSmail account available only to the requester, containing the investigation information
- in a file, sent by way of an attachment, via NHSmail to the requester's NHSmail address.

6.25. Support

6.25.1. Staff members who need support and guidance should initially contact the CITS Service Desk:

- opening hours: 08:30 – 17:00, seven days a week (out of hours emergency cover by an on-call engineer)
- telephone number: (01209 88) 1717
- e-mail (not to be used for an incident or a support call requiring urgent attention) citsservicedesk@nhs.net

6.25.2. If you have any queries about the confidentiality aspects with the information you are sending you should contact your Caldicott Guardian, Head of Information Governance or Data Protection Officer.

6.26. Retention and Destruction

6.26.1. The Trust reserves the right to retain email as required to meet its legal obligations.

6.26.2. Where the content of an email or attachments forms part of a record it is the responsibility of the staff member to ensure it is added to, and becomes part of, that record whether held in hard copy or electronic format. Attachments can be saved to folders and where the content of an email needs to be saved (i.e. evidence of comments from various sources forming a conclusion or action); it can be printed either to hard copy or electronically (Adobe Acrobat Portable Document Format, PDF).

6.26.3. Emails and attachments that do not relate to work activities or do not need to be kept as part of a record should be retained in line with the Trust Records Retention Policy.

6.27. Reporting IT Security Incidents

6.27.1. Any member of staff must report an IT security incident where they feel that there is a risk to client health, confidentiality or reputation.

6.27.2. IT security incidents should be reported to the CITS Service Desk who will ensure that any such incident reports are escalated to the IT Security Management Team.

6.27.3. Examples of incidents are:

- A lost or stolen mobile device

- misuse of NHSmail
- non-compliance with Trust policy, national policy or UK legislation
- any unauthorised access to NHSmail.

6.27.4. The IT Security Management Team will then manage the incident in accordance with the Trust's Procedure for Reporting IM&T Security Incidents

6.27.5. The incident must be logged on the Trust Incident reporting tool.

6.28. Liability

The Trust will not be liable for any financial or material loss to an individual when using their NHSmail account for personal use or when using personal equipment to access their NHSmail account.

7. Dissemination and Implementation

The Trust's Information Governance Group (RCHT)/Steering Group (CFT)/Sub Committee (NHS K) is responsible for overseeing the implementation of this Email Policy including monitoring compliance. It is responsible for ensuring it is reviewed periodically.

8. Monitoring compliance and effectiveness

8.1. The Trust has an obligation to ensure that the email system and its contents are appropriate as described in this policy.

8.2. The use of email is not private. The content of email is not routinely monitored, but the Trust reserves the right to access, read, print, or delete emails at any time.

Element to be monitored	Outgoing emails are recorded automatically to logs recording who sent the email, to whom, subject title and attachment information.
Lead	IT Security Team
Tool	Detailed information on the email content can be retrieved from NHSmail if necessary.
Frequency	Logs are created automatically when emails are sent and received. Detailed information on the contents of emails is only accessed as part of an official investigation or to resolve maintenance issues with the permission of the user.
Reporting arrangements	Breaches of this policy will be reported to the Head of Information Governance and may be passed to the appropriate line manager, HR Manager or Local Counter Fraud Specialist as appropriate.
Acting on recommendations and Lead(s)	IT Security Team
Change in practice and lessons to be shared	Required changes to practice will be identified following changes in legislation, Department for Health and IG Toolkit or Data Security and Protection Toolkit requirements and as a result in any investigations. Changes will be

	recommended to the Information Governance Committee for adoption and this will be disseminated to staff via the Document Library or staff bulletin as appropriate.

9. Updating and Review

The E-mail Policy is updated and reviewed every three years.

10. Equality and Diversity

10.1. This document complies with the Royal Cornwall Hospitals NHS Trust service Equality and Diversity statement which can be found in the 'Equality, Inclusion & Human Rights Policy' or the Equality and Diversity website.

10.2. Equality Impact Assessment

The Initial Equality Impact Assessment Screening Form is at Appendix 2.

Appendix 1. Governance Information

Document Title	Cornwall and Isles of Scilly NHS Community E-mail Policy V3.1		
Date Issued/Approved:	10th January 2020		
Date Valid From:	March 2020		
Date Valid To:	3rd October 2021		
Directorate / Department responsible (author/owner):	CITS IT Security Manager		
Contact details:	01209 318647		
Brief summary of contents	To aid the effective and appropriate use of email on Trust systems and to reduce the risk of adverse events by setting out the rules governing the sending, receiving, and storing of email; establishing Trust and user rights and responsibilities for the use of NHSmail and promoting awareness of and adherence to current legal requirements and NHS information governance standards		
Suggested Keywords:	Email, appropriate, sending, receiving, NHSmail		
Target Audience	RCHT	CFT	KCCG
	✓	✓	✓
Executive Director responsible for Policy:	Chief Information Officer		
Date revised:	10th January 2020		
This document replaces (exact title of previous version):	Cornwall and Isles of Scilly NHS Community E-mail Policy V3.0		
Approval route (names of committees)/consultation:	Information Governance Group, RCHT Information Governance Steering Group, CFT Information Governance Sub Committee,NHSK		
Care Group Manager confirming approval processes	Kelvyn Hipperson		
Name and Post Title of additional signatories	Not Required		
Name and Signature of Care Group / Directorate Governance Lead confirming approval by specialty and divisional management meetings	{Original Copy Signed}		
	Name: CITS Security Manager		

Signature of Executive Director giving approval	{Original Copy Signed}			
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Internet & Intranet	✓	Intranet Only	
Document Library Folder/Sub Folder	Information Governance			
Links to key external standards	Data Protection Act 2018 Human Rights Act 1998 common law duty of confidentiality Computer Misuse Act 1990 Environmental Information Regulations 2004 NHS Code of Practice on Confidentiality Caldicott Principles NHS Care Record Guarantee NHSmail Access Policy NHSmail Acceptable Use Policy NHSmail Access to Data Policy NHSmail Information Management Policy NHSmail Data Retention Policy			
Related Documents:	IT Security Policy Acceptable Use Policy			
Training Need Identified?	No			

Version Control Table

Date	Version No	Summary of Changes	Changes Made by *(Name and Job Title)*
Jan 2011	v1.0	Policy created	M Scallan – RCHT IG Lead
Feb 2011	v1.1	Policy amended to reflect comments made by RCHT Information Governance Committee	M Scallan – RCHT IG Lead
Feb 2011	v1.2	RCHT Policy on Policies compliant	M Scallan – RCHT IG Lead
07/07/11	v1.3	Change to reflect Cornwall NHS Community	Andrew Mann – CITS IT Security Manager
13/01/12	V1.4	Changes to include comments of Local Counter Fraud Specialist	Bev Gallagher – Head of Information Governance
23/04/12	V1.4	Minor formatting changes accepted and addition to Section 7.7 with addition of paragraphs 2 and 3.	Zoe Howard – Head of Communications

01/08/12	V1.4.1	Section 7.8 updated with minor changes following review at IGC	Bev Gallagher – Head of Information Governance
01/09/12	V1.5	Updated Appendix 1 to latest version	Andrew Mann – IT Security Manager
11/01/13	V1.6	Converted to RCHT Policy format and minor changes	Mark Scallan – IG Lead
05/03/13	V1.7	Updated from comments from Mark Scallan, Andrew Mann and Dave Watson, incorporate process for staff transferring from one organisation to another plus consistency re email and corporate records.	Simon Goodwin – Director of Health Informatics and ICT Services.
07/11/14	V1.8	Updated to include information relevant to the use of NHSmail.	Martin Price, IT Security Manager
10/11/15	V2.0	Updated to reflect migration to NHSmail	Martin Price, IT Security Manager
18/01/18	V2.1	Updated to reflect changes to national NHSmail policy and GDPR (DPA18)	Martin Price, IT Security Manager
15/01/18	V3.0	Revised following review comments	Martin Price IT Security Manager
20/01/20	V3.1	Revised following comments received from CFT	Andrew Mann IT Security Manager

All or part of this document can be released under the Freedom of Information Act 2000

This document is to be retained for 10 years from the date of expiry.

This document is only valid on the day of printing

Controlled Document

This document has been created following the Royal Cornwall Hospitals NHS Trust Policy on Document Production. It should not be altered in any way without the express permission of the author or their Line Manager.

Appendix 2. Initial Equality Impact Assessment Form

Name of the strategy / policy /proposal / service function to be assessed Cornwall and Isle of Scilly NHS Community E-mail Policy V3.1	
Directorate and service area: Health Informatics and ICT Services	**New or existing document:** Existing
Name of individual completing assessment: Martin Price	**Telephone:** 01209 318647

1. *Policy* Aim* *Who is the strategy / policy / proposal / service function aimed at?*	To ensure appropriate use of the Trust email system				
2. *Policy* Objectives*	To ensure staff, managers and the CITS organisation each understand their responsibilities for the use of the Trust email system.				
3. *Policy* – intended Outcomes*	• Staff and managers understand appropriate and inappropriate use of the Trust email system • No breaches of the Data Protection Act via misuse of the Trust email system • No patient or confidential information is compromised through the improper use of the Trust email system • Information that should be part of the corporate record is not stored within the email system • Staff report receiving less inappropriate emails				
4. *How will you measure the outcome?	Recorded incidents of misuse on Datix				
5. Who is intended to benefit from the *policy*?	The Trust and employees of the Trust				
6a Who did you consult with	Workforce	Patients	Local groups	External organisations	Other
	X				
b). Please identify the groups who have been consulted about this procedure.	**Please record specific names of groups** Information Governance Group, RCHT Information Governance Steering Group, CFT Information Governance Sub Committee, NHSK				
What was the outcome of the consultation?	Agreed				

7. The Impact
Please complete the following table. **If you are unsure/don't know if there is a negative impact you need to repeat the consultation step**.

Are there concerns that the policy **could** have differential impact on:				
Equality Strands:	Yes	No	Unsure	Rationale for Assessment / Existing Evidence
Age		**X**		

Sex (male, female, trans-gender / gender reassignment)		**X**		
Race / Ethnic communities /groups		**X**		
Disability - Learning disability, physical impairment, sensory impairment, mental health conditions and some long term health conditions.		**X**		
Religion / other beliefs		**X**		
Marriage and Civil partnership		**X**		
Pregnancy and maternity		**X**		
Sexual Orientation, Bisexual, Gay, heterosexual, Lesbian		**X**		

You will need to continue to a full Equality Impact Assessment if the following have been highlighted:

- You have ticked "Yes" in any column above and
- No consultation or evidence of there being consultation- this excludes any *policies* which have been identified as not requiring consultation**. or**
- Major this relates to service redesign or development

8. Please indicate if a full equality analysis is recommended.	**Yes**		**No**	**X**

9. If you are **not** recommending a Full Impact assessment please explain why.

Not indicated

Date of completion and submission	10th January 2020	Members approving screening assessment	Policy Review Group (PRG) **APPROVED**

This EIA will not be uploaded to the Trust website without the approval of the Policy Review Group.

A summary of the results will be published on the Trust's web site.

Appendix 3. NHSmail Mobile Device Security Policies

Category	Policy Setting	NHSmail Policy
Loss Protection	Mobile device password required	Yes
	Minimum mobile device password length	Four characters
	Maximum inactivity time lock	Twenty minutes
	Maximum fail mobile password attempts[1]	Eight
	Mobile password expiry	Never
	NHSmail password expiry	90 days
	Policy refresh interval	One hour
Data aggregation	Maximum attachment size[2]	10MB
	Maximum email body truncation size	64KB
	Maximum HTML email body truncation size	Unlimited
	Maximum email age filter	One month
Encryption	Enforces encryption at rest on devices that support this feature?	Yes

[1] The phone will be automatically wiped of all NHSmail data and restored to its default factory settings after the last failed attempt. Refer to the device's manufacturer guide for non-NHSmail data (photos, documents) stored on the device

[2] This size only applies to a mobile device. Attachments over this size will be received by your NHSmail mailbox

Appendix 4. Compatible Mobile Devices

Manufacturer	Device/Application	Supports encryption at rest?
Android	Android 6.0 (Marshmallow) and later or with Symantec Touchdown installed	Yes
Apple	iPhone 5 and later	Yes
	iPad and iPad 2 with iOS 4.3 and later	Yes
Windows Mobile	Windows Mobile 10	Yes[1]
Blackberry	OS 10 and later with ActiveSync[2] or with NotifySync 4.7 or later installed[3]	

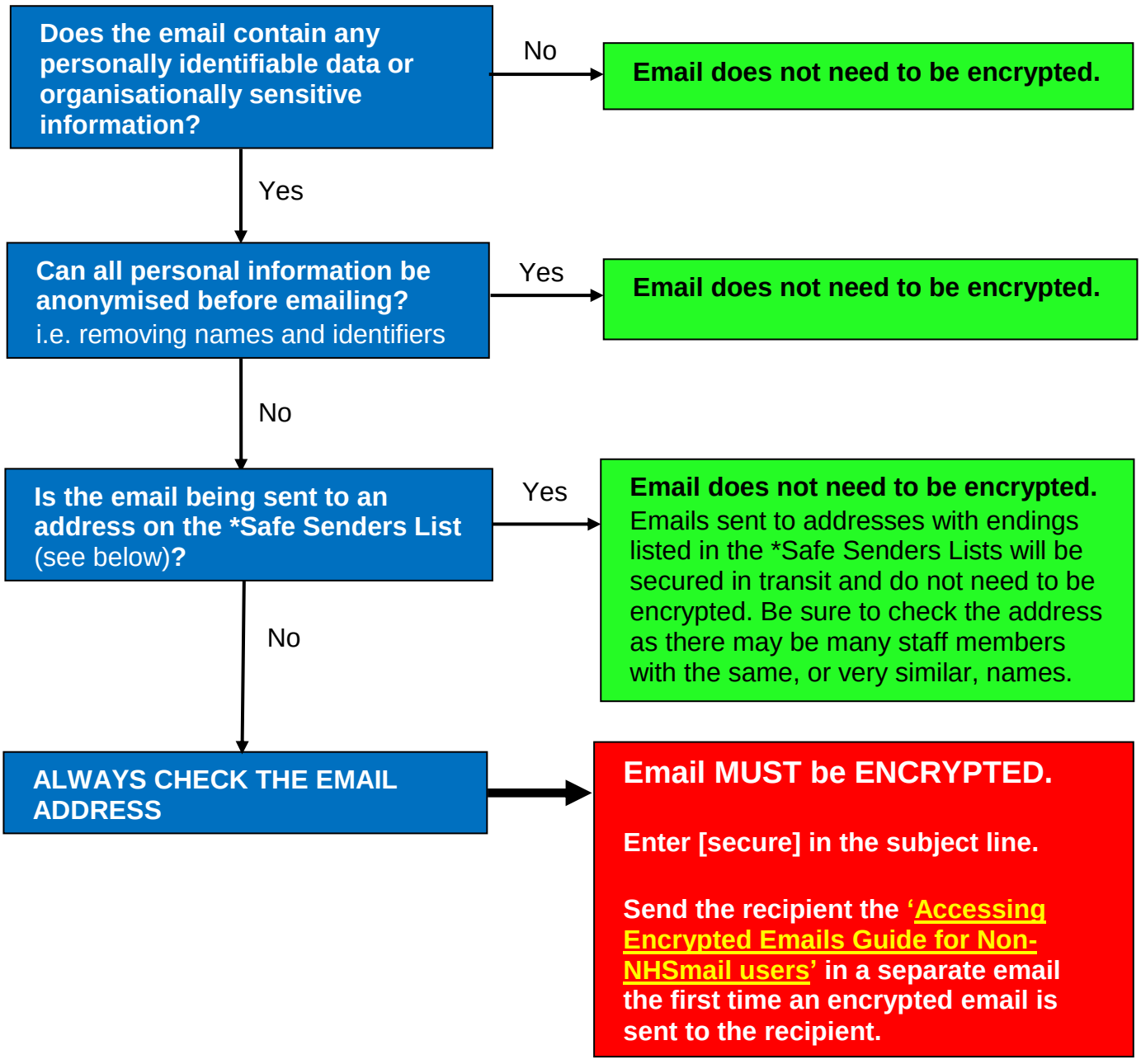
[1] Encryption may have to be manually enabled by the user. Please check with the manufacturer.

[2] Encryption will have to be manually enabled by the user. Please check with the CITS Service Desk before enabling.

[3] When running NotifySync to connect to NHSmail, native encryption at rest should NOT be switched on. If it is switched on, Contacts and Calendar will not sync and only access to email will be available.

Appendix 5. Email Encryption Decision Tree (NHSmail)

Sending information via email is a very efficient way of transferring information from one person or organisation to another. However when sending person identifiable or confidential information we must ensure that the information remains secure. Below is a decision tree to help guide users if there is a need to encrypt (make secure) email information.



* Safe Senders List:

NHS	Local Gov & Social Serv.	Police	Central Gov.	Ministry of Defence
*.nhs.net	*.gov.uk	*.pnn.police.uk	*.Parliament.uk	*.mod.uk
*.secure.nhs.uk		*.csjm.net		