Collaboration (Email, Chat and Instant Messaging) Policy

Date approved: 05 June 2026

Purpose: The purpose of the policy is to aid the effective and appropriate use of digital collaboration (using email, Office 365 or Instant Messaging apps) on NHS organisation business and to reduce the risk of adverse events by setting out the rules governing the sending, receiving and storing of data using the collaboration tools available, establishing roles and responsibilities for the use of such tools and promoting awareness of and adherence to current legislation, regulations, standards and good practice guidance.

Target audience: This policy applies to all staff members of the Cornwall and Isles of Scilly ICS member organisations.

Document author and role: Martin Price, Cyber Security Lead
Document authors contact details: 01872 250000

Document definition: Policy

Audience:
☒ Royal Cornwall Hospitals NHS Trust
☒ Cornwall Partnership NHS Foundation Trust
☒ Cornwall and Isles of Scilly Integrated Care Board

Freedom of information: Can be released under the Freedom of Information Act 2000. This document will be published on the internet and intranet.

Key words: collaboration, email, NHSmail, NHS.net Connect, Teams, 365, instant messaging, IM, Signal, WhatsApp.

Ratification

Supporting committee: Information Governance Steering Group
Approved at (if applicable): Information Governance Steering Group
Date: March 2026

Executive lead approved: Company Secretary
Date: 05 June 2026

Document library section: Information management and IT, Information technology

---

Version control summary

Version	Date	Sponsor and/or reviewer	Changes (key points) Include Section or page number.
V1.0	01/03/26	M. Price, Cyber Security Lead	V1.0 created
V1.1	20/03/26	Andrew Mann, IT Security Manager	Inactive accounts procedure updated
V2	June 2026	Philippa Harding, NHS CIOS Company Secretary	Agreed at the March 2026 Information Governance Steering Group and approved by the Company Secretary in June 2026.

This document replaces:

- Cornwall and Isles of Scilly NHS Community E-mail Policy, Microsoft Office and N365 Applications Policy

Contents

1. Introduction 6
2. Scope 6
3. Definitions and glossary 7
4. Ownership and responsibilities 9
5. Standards and practice 13
6. Related legislation, national and local guidance 28
7. Training requirements 29
8. Implementation 29
9. Document monitoring arrangements 29
10. Environmental sustainability 29
11. Updating and review 30
12. Equality and diversity 30
Appendix 1: Equality Impact assessment Form 31

Data Protection Act 2018 (UK General Data Protection Regulation Legislation)

The NHS organisation has a duty under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 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 consent may be required. This must be explicit, informed, and documented. Opt out cannot be relied on; it must be opted in.

The Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 are applicable to all staff members; this includes those working as contractors and providers of services.

For more information about obligations under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679, contact the Information Governance Team.

1. Introduction

1.1. The use of Office 365, including Outlook and Teams and other instant messaging apps are recognised methods for day to day internal and external communication by NHS organisations. They can be of great benefit to the NHS when used appropriately. Their 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 electronic collaboration is with the intended recipient and that the content is appropriate to be sent in the format selected.

1.2. Email, Teams chat or other instant messaging are not always the best way to communicate information as such methods of electronic collaboration can often be misunderstood. The pure volume of messages can also be prohibitive to effective communication. Emails, chats and messages should be treated with the same level of attention that is given to drafting and managing formal letters and reports. As well as taking care over how such messages are written, messages should be managed appropriately after they have been sent or received.

1.3. This policy is based on current legislation, regulations and good practice guidance. Staff members' duty to handle organisation and personal identifiable data appropriately arises out of common law, legal obligations, staff employment contracts, and professional obligations.

1.4. This policy clearly sets the expectations in the use and management of email, Teams or other instant messaging systems, hereafter known as collaboration tools, including accessing personal collaboration tools on ICS member organisations' equipment.

1.5. Staff members should ensure that they are familiar with the content of this policy and use it as a point of reference when undertaking any electronic collaboration.

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

2. Scope

This policy applies to, but is not limited to employees, non-executive directors, contractors, agency staff members, researchers, trainees, students and volunteers.

It describes the standards and practices with regards to electronic collaboration and is relevant specifically to the use of Microsoft Outlook, Microsoft Teams and other Microsoft 365 applications. It does not necessarily and specifically relate to other public instant messaging or external instant messaging systems or apps, such as WhatsApp, although the principals of good practice remain the same.

3. Definitions and glossary

3.1. **Collaboration**: A collaborative system through digital devices which allows users to exchange emails, messages, chats and information online by way of workstation or mobile device.

3.2. **Collaboration Tools**: Software or apps that offer email, messaging and chat as well as file sharing, contextual assistance, shared access to calendars and voice and video calls for one-on-one and group calls and meetings.

3.3. **Cornwall and Isles of Scilly Integrated Care System (C&IoS ICS)**: Comprised of the Cornwall and Isles of Scilly Integrated Care Board (C&IoS ICB), the Royal Cornwall Hospitals NHS Trust (RCHT), the Cornwall Partnership NHS Foundation Trust (CFT), Kernow Health (KHCIC) and the GP practices across Cornwall and the Isles of Scilly, collectively the Cornwall and Isles of Scilly ICS member organisations, the Cornwall and Isles of Scilly ICS members.

3.4. **Cornwall CoIN**: A managed Community of Interest Network (CoIN). This wide area network links all the computers across all Cornwall and Isles of Scilly ICS member organisations sites with the national Health and Social Care Network.

3.5. **Cornwall IT Services (CITS)**: The IT department of the Royal Cornwall Hospitals Trust. CITS provide comprehensive digital services support for the C&IoS ICS members.

3.6. **Cornwall Cyber Security Operations Centre (CSOC)**: Resourced by CITS and aims to predict, prevent, detect, respond to and recover from cyber security incidents based on the monitoring of cyber security tools, analysis of the data output from those tools and other sources and using highly credible threat intelligence.

3.7. **Credentials**: A user identity, in this context, usually a username, an email address or other unique identifier and password combination that allows a staff member to access collaboration tools.

3.8. **Data Protection Impact Assessment (DPIA):** a process designed to help systematically analyse, identify and minimise the data protection risks of a project

or plan that is designed to assess and demonstrate compliance with data protection obligations.

3.9. **Data Security and Protection Toolkit (DSPT)**: The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against both the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) and the National Data Guardian's 10 data security standards.

3.10. **Digital Services**: Comprised of Cornwall IT Services, ICB Digital Services and Kernow Health Digital Services.

3.11. **Ghost Account**: A ghost NHS.net Connect account, or generically named account is a person NHS.net Connect account that has been named to reflect the purpose for which it was created, e.g. trelawney.reception@nhs.net.

3.12. **Health and Social Care Network (HSCN)**: A data network for health and care organisations that provides the underlying network arrangements to help organisations access systems easily and smoothly and share information more reliably, flexibly and efficiently.

3.13. **Information Commissioner's Office (ICO)**: The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

3.14. **Instant Messaging**: Instant messaging, or chat, is the exchange of near-real-time messages through an instant messaging app, e.g. Microsoft Teams. Instant messaging usually take place between two users in a private, back-and-forth style of communication.

3.15. **Local Administrators**: The prime contacts responsible for the administration of local NHS.net Connect accounts. They will help with resetting passwords (when the self-service password reset cannot be utilised) setting up shared mailboxes, and authorising distribution lists

3.16. **Microsoft Teams**: Microsoft Teams is a team collaboration application developed by Microsoft as part of the Microsoft 365 family of products, offering instant messaging and video conferencing.

3.17. **Mobile Device**: A personal computer small enough to hold and operate in hand, typically battery-powered with a flat-panel display and one or more built-in input devices, such as a touchscreen or keypad.

3.18. **Multi-Factor Authentication (MFA)**: An electronic authentication method in which a user is granted access to a system only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

3.19. **Must**: This word, or the terms "**required**" or "**shall**", mean that the definition is an absolute requirement of this policy.

3.20. **National CSOC**: Resourced by NHS England and follows the same aims as the Cornwall CSOC at a national level.

3.21. **NHS.net Connect**: NHS.net Connect (formerly NHSmail) is the national platform for NHS email, communication and collaboration. It provides staff with secure access to email, chat, online meetings, file sharing and more.

3.22. **Resource Account**: A 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 sending and receiving emails on behalf of the team. All staff members who have access to the resource account can send emails 'on behalf' of the account.

3.23. **Should**: This word, or the adjective "**recommended**" mean that there may be valid reasons for not applying the requirement, but the full implications must be understood and carefully considered.

3.24. **Senior Information Risk Officer (SIRO)**: Typically, a member of the executive leadership team, retains overall accountability for information governance and is the overall owner of information risk within the organisation.

3.25. **Signal**: An external instant messaging service. It allows users to send text, voice messages and video messages.

3.26. **Telegram:** An external instant messaging service. It allows users to send text, voice messages and video messages

3.27. **User**: Any individual or system process authorised to access collaboration tools and, therefore, includes generic accounts and service accounts.

3.28. **WhatsApp**: An external instant messaging service. It allows users to send text, voice messages and video messages.

4. Ownership and responsibilities

4.1. Ownership

4.1.1. The ICS members provide access to collaboration tools to staff members primarily for use in their:

- work duties
- work related education and training purposes
- work related research purposes.

4.1.2. The ICS members allow personal use of collaboration tools provided this does not interfere with the performance of duties, those of other staff or contractors or the business of the organisation in general. Personal access to collaboration tools can be limited or denied by the line manager. Staff members must act in accordance with NHS organisation policies and their manager's locally imposed restrictions.

4.1.3. No staff member has the right to access to collaboration tools. On this basis the inappropriate use or abuse of collaboration tools may result in access being withdrawn or amended.

4.1.4. The organisation reserves the right to remove or amend access to collaboration tools at any time in order to protect and preserve the integrity and confidentiality of the system.

4.2. Responsibilities

4.2.1. Responsibilities of the Chief Information Officer

The Chief Information Officer (CIO) has overall accountability for the implementation of collaboration tools across the C&IoS ICS and for ensuring the continued, safe use of this and public and external instant messaging systems.

4.2.2. Responsibilities of the SIRO

The SIRO has accountability for ensuring that effective systems and processes are in place to manage the risks relating to the use of collaboration tools, retains overall accountability for information governance and is the overall owner of information risk within the organisation.

4.2.3. Responsibilities of Managers

4.2.3.1 Line managers are responsible for:

- ensuring that the staff members that they manage are aware of this policy and their individual responsibilities for complying with it

- ensuring their staff members are equipped to fulfil those responsibilities including meeting specific and generic training needs through personal development plans

4.2.3.2 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 providing access to collaboration tools
- movers/leavers – managers should work with a staff member that leaves or changes role to transfer any organisation information stored within their NHS.net Connect account to either an appropriate person or shared work area, for purposes of business continuity, ensuring that personal identifiable and sensitive or confidential data is deleted from the mover's/leavers account so that the NHS.net Connect account can be made available for the staff member's next assignment with the same or a different NHS organisation.

4.3. Responsibilities of CITS

CITS are responsible for:

- implementing Microsoft collaboration tools in accordance with good practice
- ensuring all NHS.net Connect accounts for those staff members who have left or moved roles are disabled or modified in a timely manner
- adhering to the NHS.net Connect Access to Data Procedure to facilitate access to data stored in Microsoft Office 365 on behalf of the ICS members when dealing with formal investigations
- facilitating access in line with good practice guidance, where there is a critical business need, to provide proxy access to a staff member's NHS.net Connect mailbox during long term absence
- documenting and assessing any risks relating to the use of collaboration tools as necessary.

4.4. Groups and committees

4.4.1. Responsibilities of the Information Governance Group/Steering Group/Sub-Committee

The organisation's Information Governance Group/Sub Committee/Steering Group, herein known as the Information Governance Group, is responsible for:

- approving the policy
- ensuring that it is disseminated to all relevant staff members.

5. Standards and practice

5.1. New Starters

5.1.1. The CITS Service Desk receive regular reports from the Recruitment Team to identify new employees and their start date.

5.1.2. The information contained within these reports is used to provision the relevant NHS.net Connect account in advance of the start date provided.

5.1.3. The new starter should contact the CITS Service Desk on or after their start date to activate their NHS.net Connect account.

5.2. Movers and Personal Information Changes

5.2.1. When a staff member changes roles within the NHS organisation 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 NHS.net Connect account details based on the information provided.

5.2.2. The personal information that is typically recorded on NHS.net Connect and that can be changed is:

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

5.3. Changes to Employment Status

5.3.1. Upon receipt of the notification the CITS Service Desk will suspend the NHS.net Connect account.

5.3.2. If proxy access to the NHS.net Connect account is required whilst the user account is suspended the manager should request access in the absence of a staff member.

5.3.3. Where proxy access is provided in the absence of a staff member the staff member must be informed of the reason for gaining proxy access and the period of proxy access that occurred on their return.

5.3.4. The NHS.net Connect 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.

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

- Maternity.
- Long-term sickness.
- Suspend assignment.
- Suspended with pay.
- Suspend no pay.
- Suspend contingent assignment.

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

5.4. Official Investigations

5.4.1. When an employee 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 NHS.net Connect is disabled, if appropriate, in a timely fashion and maintained consistently with the information available to the manager. The manager should consider whether the NHS.net Connect account should be disabled, resulting in an autoreply informing senders of this, that may lead to speculation or rumours, or whether to request that a randomly generated password is applied to the active account to prevent the potentially unwanted autoreply.

5.4.2. When dealing with some official investigations, the organisation may require access to NHS.net Connect data held in the name of one or more of their staff members.

5.4.3. These requests typically fall into three categories:

- disciplinary investigations or other organisation investigations including clinical and non-clinical
- investigations by, or on behalf of the police, the NHS Counter Fraud Service, or other bodies such as these
- Subject Access Requests (SARs) - Individuals have the right to access their personal data under data protection legislation.

5.4.4. Any official investigations will be carried out in accordance with UK 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.

5.4.5. CITS will only accept initial investigation requests relating to a staff member's NHS.net Connect account from the relevant People Partner, the appointed investigating officer, the local counter fraud specialist, or the local security management specialist.

5.4.6. Investigation requests must be sent to the CITS Service Desk using the specific offering, Employee Audit Data. The communication must include the explicit permission of one of the requesting officers as outlined above.

5.4.7. The organisation 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, always maintaining confidentiality.

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

- the name of the staff member and their NHS.net Connect address
- what information is required, based on information published in NHS.net Connect policy):
  - the contents of a mailbox at a point in time
  - copies of messages sent and/or received (whether deleted by the staff member or not) and Teams one-to-one chats to or from that mailbox in the last 180 days
  - a journal of all emails sent or received in the last two years (date, time, sender, recipient, subject).

5.4.9. Once a correctly formed request has been received CITS will seek explicit permission from one of the following before submitting the request to NHS England for authorisation and onward submission to NHS.net Connect:

- the Chief People Officer or the Chief Executive Officer (or equivalent).

5.4.10. No service level is associated with official investigation requests, and all requests will be dealt with on a 'first come, first served basis'.

5.4.11. Once NHS.net Connect have processed the request, the information will be provided to CITS in the form of a link to download an Outlook data file that can be added to an existing Outlook installation to provide access to the relevant contents.

5.4.12. It should be noted that requests relating to an official investigation may return all emails pertaining to the investigation, including emails (or a summary of emails)

that have been deleted by the staff member. Emails, messages or chats that have been marked as personal may not exempt them from discovery as part of an official investigation or being used as supporting evidence in such an investigation.

5.4.13. Requests for access to NHS.net Connect data that is subject to public inquiries or other investigations in accordance with the Inquiries Act 2005 are not governed by national procedures published by NHS.net Connect or this policy.

5.5. Proxy Access

5.5.1. There is no right for a manager to demand access to a staff member's NHS.net Connect account. Where necessary, staff members may provide proxy access to their NHS.net Connect account to colleagues or their manager for legitimate business purposes.

5.5.2. Where a colleague has been given the authorisation to send emails from another NHS.net Connect account, it should be made clear within the email, who the email author is.

5.6. Access in the Absence of a Staff Member

5.6.1. Staff members should ensure that during periods of planned absence, they have made arrangements for proxy access to their NHS.net Connect 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 a staff member's NHS.net Connect account for the purposes of business continuity.

5.6.2. Where proxy access is provided in the absence of a staff member the staff member must be informed of the reason for gaining proxy access and the period of proxy access that occurred on their return.

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

5.6.4. Access to another staff member's NHS.net Connect account should have the support from:

- the organisation's Chief People Officer and;

- the Chief Medical Officer, where there may be evidence that the NHS.net Connect account may contain confidential or personal identifiable data that should only be seen by a limited group of staff members.

5.6.5. It is recommended that an out of office message is added to the NHS.net Connect account of the absent staff member informing senders to re-send the information to an alternative NHS.net Connect address so that business continuity can be maintained.

5.7. Secondments

5.7.1. Staff going on secondment within the organisation should be treated as a mover.

5.7.2. Staff going on secondment to another NHS organisation should be treated as a leaver and joined to the new organisation.

5.8. Temporary Staff

5.8.1. When considering whether to provide access to NHS.net Connect for a temporary staff member, the following points should be considered:

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

5.9. Long-Term Access Assignments

5.9.1. 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.

5.9.2. The temporary staff member will be provided with access to NHS.net Connect or their personal information on NHS.net Connect will be updated to reflect their current assignment.

5.9.3. 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 NHS.net Connect, if appropriate.

5.10. Staff Members Not Directly Employed by the Organisation

5.10.1. The organisation acknowledges that there are some instances where staff members are not directly employed.

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

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

5.10.3. Staff members not directly employed by the organisation that require access to an NHS.net Connect account should seek appropriate sponsorship from the appropriate manager within the organisation, who should submit a request via the CITS OnForm system.

5.10.4. Staff members not directly employed by the organisation should notify the CITS Service Desk of changes to personal information along with approval from the sponsoring manager.

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

5.11. Generic Accounts

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

5.11.2. Where there is a genuine need for a generic NHS.net Connect account, this should be requested by the staff member to the manager. At this point the request is verified prior to the request being forwarded to the CITS Service Desk for the NHS.net Connect account to be created.

5.12. Resource Accounts

5.12.1. Resource accounts must be set up by the CITS Service Desk who will also set the access permissions. Resource account names should always be prefixed by the owning organisation's "short code", e.g. ciosicb.accountname@nhs.net.

5.12.2. Resource accounts are specifically linked to the organisation and cannot be migrated to another organisation using the same process as for a named individual staff member's account.

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

5.13. Ghost Accounts

5.13.1. 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.

5.13.2. If the ghost 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.

5.14. Dual Employment

5.14.1. Where a staff member has dual employment with two, or more, NHS organisations within the C&IoS ICS the substantive or earliest employer should determine which organisation their named NHS.net Connect account will be associated with. Multiple NHSmail accounts for the same staff member should not be created.

5.14.2. It is the dual-employed staff member's responsibility to manage collaboration tool settings to ensure that emails, chats and messages relating to separate NHS organisations are handled appropriately and that any information contained within digital collaboration is separated accordingly.

5.15. Password and MFA Resets

5.15.1. Staff members who have forgotten their NHS.net Connect password should follow the instructions on Self-Service Password Reset Portal to complete a self-service password reset.

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

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

5.16. Inactive Accounts

5.16.1. NHS.net Connect accounts will be regularly monitored to identify inactive accounts. Any named NHS.net Connect accounts (including ghost accounts) that are found to be inactive for longer than 30 days will be marked as inactive. After 60 days of inactivity, an inactive account will be deleted. After 90 days of inactivity a deleted account will be permanently deleted.

5.16.2. Any resource accounts that are found to be inactive will be handled in the same way.

5.16.3. 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.

5.16.4. Pre-provisioned accounts that are not activated by the staff member within 90 days of creation will be deleted automatically.

5.17. Compromised Accounts

5.17.1. If the national CSOC identify that an NHS.net Connect account has been compromised, they will disable the account and send an email alert to the Local Administrators (LA).

5.17.2. When the CITS Service Desk are informed that an NHS.net Connect password has become known to another staff member or the account has been accessed in an unauthorised manner they will disable the account and report this as an incident to the Cornwall CSOC.

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

5.18. Leavers

5.18.1. The CITS Service Desk will receive regular scheduled ESR reports to identify staff members directly employed within C&IoS ICS that have left.

5.18.2. This information will be used to disable the relevant NHS.net Connect account for a period of 30 days.

5.18.3. After 30 days, if the NHS.net Connect account has not been ‘joined’ to a new NHS organisation then the account will be deleted.

5.19. Managing Collaboration

5.19.1. Collaboration tools are not a records management system. Where the contents of an email, message or chat may be needed in the future it is the responsibility of the staff member to ensure that it is stored appropriately within the corporate or clinical records system.

5.19.2. Storage space per user on NHS.net Connect is limited to a maximum allocation determined by NHS.net Connect. Exceeding the allocated space could result in the corruption and loss of emails, messages or chats.

5.20. Use of Collaboration Tools

5.20.1. Staff members should use collaboration tools only when it is appropriate to do so and not as a substitute for verbal communication. Emails, messages and chats should be worded with care because voice inflections cannot be picked up and it can be difficult to interpret the ‘tone’.

5.20.2. Using a collaboration tool should be regarded as a formal method of communication and care should be taken when composing an email, message or chat.

5.20.3. Collaborations must not include anything that would offend or embarrass any reader or would embarrass the organisation if it found its way into the public domain.

5.20.4. Write all emails, messages or chats on the assumption that they may be read by others, particularly people who do not normally work for the organisation, such as temporary staff. Emails, messages and chats can be easily forwarded on and may be read by unintended recipients.

5.20.5. Limit the number of recipients the email, message or chat is sent to and only ever as many recipients as is necessary. All staff members with access to NHS.net Connect have a responsibility to not overload other staff members with irrelevant emails, messages or chats and not to put pressure on recipients by copying in or including ‘people with authority’ unnecessarily.

5.20.6. A concise and meaningful title should be included wherever possible in all collaborations to indicate the content. This will assist the recipient in prioritising the opening of email, messages and chats.

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

5.20.8. Where important information has been sent using a collaboration tool, confirmation of receipt must be obtained either using the same collaboration tool or by a follow up telephone call.

5.20.9. Staff members must access NHS.net Connect regularly and respond to emails, messages and chats in a timely manner.

5.20.10. Staff members should indicate when they are not able to respond to emails, messages or chats (for example, when on annual leave) by using the tools within Office 365 (such as an 'out of office' notification).

5.20.11. Inappropriate use may result in poor communication, impede the function of the organisation's network, impede the effective functioning of NHS.net Connect, or compromise the security of the system.

5.20.12. Instant messaging may be considered as a very convenient method of keeping in touch in both work and personal lives and business and personal use may be blurred with public or external instant messaging app, such as WhatsApp, Signal or Telegram, that are easy to download and use for both business and personal use. However, the use of instant messaging for NHS business use has some additional standards and practice that must be adhered to in order to help balance the convenience of a public instant messaging app with safe and effective use.

5.20.13. Microsoft Teams is licenced and available for use on both corporate and personally owned devices and should be the default choice at work, particularly for chats involving personal identifiable information, sensitive clinical information or confidential NHS information.

5.20.14. Where it is not practical, or possible, to access Microsoft Teams, particularly on a personal mobile device, the staff member should consider carefully what information may be shared on public instant messaging apps and whether the use case has been approved by the organisation.

5.20.15. Staff members using a public instant messaging app, particularly to share personal identifiable information, sensitive clinical information or confidential NHS information should:

- use Microsoft Teams to transmit NHS information wherever possible
- use a public instant messaging app in alignment with all relevant guidance, procedures, policies, codes of practice, regulations and legislation
- handle all medical records in line with the GMC Code of Confidentiality.

5.20.16. Staff members using a public instant messaging app should not:

- transmit NHS information without confirmation that the use case has been approved by the organisation
- store the only copy of clinical decisions in Teams or a public instant messaging app
- use any messaging app, including Microsoft Teams, as the formal medical record
- share personal identifiable information, sensitive clinical information or confidential NHS information with anyone using Teams or a public instant messaging app that does not have the right to view it.

5.21. Legal Requirements

5.21.1. The use of collaboration tools must comply with UK legislation and regulations, adhere to national policies and codes of conduct, as well as local rules, policies and procedures.

5.21.2. Staff members must not use collaboration tools for any purpose that conflicts with their contract of employment.

5.21.3. Emails, messages and chats have the same legal status as any written document and must be disclosed in legal proceedings if relevant to the issues. The content of any emails or any one-to-one Teams chats may be disclosed as part of a Subject Access Request under the Data Protection Act 2018, the Freedom of Information Act 2000 or the Environmental Information Regulations 2004. On this basis, the author must ensure that the content, style and language used is appropriate.

5.22. Security

5.22.1. Credentials for NHS.net Connect must be kept confidential, for the staff member's own personal use and not shared with others for business continuity purposes or otherwise.

5.22.2. Digital services staff members or NHS.net Connect staff members will never ask a staff member to divulge their password or their MFA code.

5.22.3. Sharing passwords, MFA codes or access to collaboration tools may lead to a data security breach. Where it has been identified that NHS.net Connect credentials may have been breached, the Password and MFA Resets section of this policy should be referred to.

5.22.4. NHS.net Connect passwords must be changed annually, be self-selected and unique to the staff member and meet the NHS.net Connect password policy:

- minimum length of ten characters without requiring a mix of upper case, lower case, numbers and symbols
- must not match previous four passwords
- must not be detected as a weak password, previously publicly breached (e.g. Password123, Cornwall25)
- must not be detected as a previously compromised and publicly breached password
- must not contain staff member's first or last name.

5.22.5. NHS.net Connect passwords should also meet these additional criteria:

- not easy to guess (avoid family members' or pet's names, make and model of car, telephone numbers, etc.)
- avoid the use of single dictionary words
- try to use passphrases, constructed from three random dictionary words (e.g. Apple Penny Table).

5.22.6. If a mobile device has been configured to access NHS.net Connect, the device will have additional security controls applied to it to minimise the risk of a data security breach.

5.22.7. Staff members should logout of NHS.net Connect when they have finished using it and must lock their workstation when leaving it, for example, to make a cup of tea or to go for lunch.

5.22.8. When accessing NHS.net Connect it is the staff member's responsibility to ensure that emails, messages and chats cannot be viewed by anyone not authorised to do so.

5.22.9. Staff members should ensure that, when downloading email attachments or files shared in Teams chats or instant messages, they are saved to a secure location and that clinical decisions are transferred to the formal record as soon as possible.

5.22.10. All medical records shared using email, messages or chat should be handled in line with the General Medical Council (GMC) Code of Confidentiality and the Records Management Code of Practice for Health and Social Care 2016.

5.22.11. Emails, messages or chats containing identifiable, confidential or sensitive organisation information must not be shared with anyone not authorised to view it or distributed using personal web-based email accounts or public instant messaging systems, such as WhatsApp, Signal or Telegram.

5.23. Personal Use

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

5.23.2. Special care should be taken when using an NHS.net Connect account to send personal emails, messages or chats as they will be sent from the organisation and, therefore, may be, incorrectly, assumed to be sent on behalf of the organisation rather than from the staff member personally. This is of particular importance when collaborating with statutory bodies or formal establishments where it would be easy to misinterpret the collaboration as a formal communication from one organisation to another.

5.23.3. Staff members should only use their NHS.net Connect account to register with authorised social media sites if they have been approved to be acting on behalf of the NHS organisation. Posting or replying on social media sites and making informal suggestions or giving advice using an NHS.net Connect account could be perceived as formal NHS advice from the organisation. In general, when registering for social media sites, staff members should use a personal web-based email address.

5.23.4. Staff members should be aware that marking an email, message or chat as personal may not exempt it from discovery or being used as supporting evidence in an official investigation and such collaboration may be accessible by colleagues or the line manager in the event of access being required as part of business continuity as a result of long term sickness, for example.

5.24. Misuse of the System

Staff members must not

- use their NHS.net Connect 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 inappropriate or malicious content
- send email messages from another staff member's NHS.net Connect account using proxy access without it being clear the account owner has not been the author of the content
- send global emails to ALL staff outside of agreed processes for such communications

- use their NHS.net Connect account for political lobbying.

5.25. Sending and Receiving Attachments

5.25.1. Consider alternative ways of making documents available to other staff members, such as providing links to shared folders or saving files in Teams channels.

5.25.2. Potentially harmful file types and extensions cannot be sent as attachments across NHS.net Connect. These include executable application files, screen savers, certain audio, movie and video files, script files, and Windows registry files.

5.25.3. Password protected and encrypted attachments cannot be scanned for malicious content by NHS.net Connect. It is the responsibility of the staff member to confirm that such attachments are safe before opening them.

5.25.4. Additional rules apply to compressed (zip) files sent as attachments via NHS.net Connect in terms of the size and number of embedded layers within the compressed file.

5.26. Confidential, personal identifiable or sensitive information

5.26.1. It is the staff member's responsibility to ensure that the correct recipient has been selected when sending confidential, personal identifiable or sensitive information.

5.26.2. Such information should not be sent unless it is part of an approved data flow for which a DPIA exists.

5.26.3. Staff members should not store the only copy of clinical decisions in a collaboration tool or use either as the formal medical record.

5.26.4. Care should be taken to avoid downloading attachments containing NHS information to the local disk of a CITS PC or a personal PC and files containing NHS organisation information should not be permanently stored on the local disk of a CITS PC or personal PC.

5.26.5. Whilst emails sent to and received from NHS.net connect addresses are secured using well-configured encryption, the links between NHS.net Connect and other email addresses may not be protected with similar, well-configured encryption. To ensure that such encryption is applied, staff members should include the phrase [secure] in the subject of any emails when sending confidential, personal identifiable or sensitive information to recipients outside of NHS.net Connect.

5.26.6. Staff members may be required to collaborate on particularly sensitive information and may wish to agree a pseudonym, e.g. patient's initials, that will enable the subject to be identifiable between the sender and the recipient in any collaboration, particularly when referenced in the subject field.

5.27. Support

5.27.1. Staff members who require IT support and guidance should initially contact the CITS Service Desk.

5.27.2. Queries or questions relating to the confidentiality aspects of the information being sent should be referred to the Caldicott Guardian, Head of Information Governance or Data Protection Officer.

5.28. Retention and Destruction

5.28.1. The organisation reserves the right to retain records of collaboration as required to meet its legal obligations.

5.28.2. Where the contents of an email, chat or instant message forms part of a record, it is the responsibility of the staff member to ensure that it is added to and becomes part of that record, whether held in hard copy or digital format. Attachments may be saved to shared folders. Where the content of an email needs to be saved it may be printed to hard copy or digitally in Adobe Acrobat Portable Document Format (PDF). The content of a Teams chat or an instant message may be copied and pasted into another document and saved to a shared folder or printed. Care should be taken to ensure that the date and time of the chat or instant message is recorded along with the sender and recipients.

5.28.3. Emails, attachments, chats and instant messages that do not relate to organisation business or do not need to be retained as part of a record should be retained in line with the organisation's records retention policy.

5.29. Reporting Data Security Incidents

5.29.1. A data security incident must be reported where it is felt that there is a risk to a patient's health, confidentiality, the integrity or availability of information or the reputation of the organisation.

5.29.2. Data security incidents should be reported to the CITS Service Desk, who will escalate it to the cyber security management team.

5.29.3. Examples of incident are:

- a lost or stolen device
- misuse of or unauthorised access to a collaboration tool
- non-compliance with organisation policy, national policy, UK regulations or legislation.

5.29.4. The cyber security management team will manage the incident in accordance with the CITS internal standard operating procedures for managing incidents and ensure that the incident is escalated to the relevant head of information governance.

5.29.5. The Head of Information Governance will determine whether the incident should be reported to the ICO, the Department of Health and Social Care and NHS England using the tool provided in the DSPT.

5.29.6. A breach of personal data must be notified by the Head of Information Governance within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, those impacted must be informed without undue delay.

5.30. Liability

The organisation will not be liable for any financial or material loss to an individual when using an NHS.net Connect account for personal use or when using a personal device to access NHS.net Connect.

6. Related legislation, national and local guidance

Links to key external standards:

- Data Protection Act 2018
- Human Rights Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- Confidentiality: NHS Code of Practice - GOV.UK
- The Caldicott Principles - GOV.UK
- Access Policy – NHSmail Support
- Acceptable Use Policy – NHSmail Support
- Access to Data Procedure – NHSmail Support
- Data Retention and Information Management Policy – NHSmail Support
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

7. Training requirements

None.

8. Implementation

The individual organisations' Information Governance Group are responsible for overseeing the implementation of this policy, including monitoring compliance. It is responsible for ensuring it is reviewed periodically.

9. Document monitoring arrangements

Information category	Detail of process and methodology for monitoring compliance
Element to be monitored	All emails and Teams one-to-one chats are retained by NHS.net Connect for 180 days and a summary of emails recording the sender, recipient, date time and subject is also retained automatically.
Lead	Cyber Security Managers
Tool	NHSmail Forensic Discovery
Frequency	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)	Cyber Security Managers
Change in practice and lessons to be shared	Required changes to practice will be identified following changes in legislation, Data Security and Protection Toolkit requirements and as a result in any investigations. Changes will be recommended to the Information Governance Group for adoption, and this will be disseminated to staff via the Document Library or staff bulletin as appropriate.

10. Environmental sustainability

The Cornwall and Isles of Scilly ICS member organisations are committed and obligated to reduce their environmental impacts. Healthier outcomes can be achieved for people,

the planet and pounds by conducting our activities in a more environmentally sustainable manner

11. Updating and review

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

12. Equality and diversity

This document complies with the Cornwall and Isles of Scilly member organisations' equality and diversity statements. The statements can be found in the RCHT Equality Diversity And Inclusion Policy, CFT Equality, Diversity and Inclusion Statement and Equality and diversity - NHS Cornwall and Isles of Scilly

The initial equality impact assessment screening form is at Appendix 1.

Appendix 1: Equality Impact assessment Form

Title of policy or document for assessment: Collaboration (Email, Chat and Instant Messaging) Policy

Document library section: Health Informatics and ICT Services

Is this a new or existing document? New

Date of assessment:

Person responsible for the assessment: Martin Price

What is the main purpose of the document?
To ensure staff members understand their responsibilities for collaborating using email, instant messaging and chat.

Who is affected by the document?
☒ Staff ☐ Patients ☐ Visitors ☐ Carers ☐ Other ☐ All

The document aims to improve access, experience and outcomes for all groups protected by the Equality Act 2010.

Concerns
Are there concerns that the procedural document could have a differential impact on the following areas?
If a negative impact has been identified, please complete a full EIA by contacting the Equality, Diversity, and Inclusion Team. For RCHT please contact rcht.inclusion@nhs.net, for CFT please contact cft.inclusion@nhs.net, for CIOS ICB, please contact ciosicb.corporategovernance@nhs.net.

Concern area	Response	If yes, what existing evidence (either presumed or otherwise) do you have for this?
Age	☐ Yes ☒ No	
Disability	☐ Yes ☒ No	
Sex	☐ Yes ☒ No	
Gender reassignment	☐ Yes ☒ No	
Pregnancy and maternity	☐ Yes ☒ No	
Race	☐ Yes ☒ No	
Religion and belief	☐ Yes ☒ No	

Concern area	Response	If yes, what existing evidence (either presumed or otherwise) do you have for this?
Sexual orientation	☐ Yes ☒ No	
Marriage and civil partnership	☐ Yes ☒ No	
Groups at risk of stigma or social exclusion such as offenders or homeless people	☐ Yes ☒ No	
Human rights	☐ Yes ☒ No	

Are there any associated objectives of the document? If yes, what existing evidence (either presumed or otherwise) do you have for this?
None

Signature of person completing the equality impact assessment:
Name: Martin Price
Date: 6 November 2025