Joint Policy for Cumbria Partnership Foundation Trust & North Cumbria University Hospital NHS Trust

Policy Title: Joint Email Policy

Reference	POL/IG/011
Version	1.0
Date Ratified	19/03/2019
Next Review Date	March 2022
Accountable Director	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)
Policy Author	Trust Information and Cyber Security Officer

Please note that the Intranet / internet Policy web page version of this document is the only version that is maintained.

Any printed copies or copies held on any other web page should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Policy On A Page

SUMMARY & AIM

This Policy supports the Trusts in complying with information legislation that applies to e-mail, including, but not limited to, the General Data Protection Regulations, Data Protection Act 2018, Freedom of Information Act 2000 and Regulation of Investigatory Powers Act 2000. In addition to complying with legislation, both Trusts will ensure that appropriate business records are maintained for audit and accountability purposes. Management of e-mail will be undertaken in such a way that staff are treated with respect and that their rights are not violated.

The aim of this Policy is to ensure all staff members use Trust email effectively and properly in pursuit of Trust statutory obligations.

TARGET AUDIENCE:

- All Trust employees, consultants, third parties, contractors and temporary workers using Trust e-mail systems or accounts, regardless of intended use.

TRAINING:

- Employee Induction
- Mandatory Data Security Awareness training using the Trust TNA eLearning programme option: 261 – 0000 Data Security Awareness Level 1

KEY REQUIREMENTS

1. Users must always comply with the rules laid down in this Policy when using Trusts' email facilities.

2. Users must also remember that it is not just in emails, but in verbal and written communication that risk is involved and breaches may occur.

3. Users must only use their work email address in support of the business requirements of the Trusts.

4. Managers must ensure all staff members are aware of and in compliance with this Policy.

5. Managers must ensure that any potential disciplinary action with regard to the use or misuse of email is investigated with this Policy in mind.

6. Managers must also ensure that their users are aware of and have read the Email Use Guidelines in Appendix 1.

TABLE OF CONTENTS

1. INTRODUCTION 4
2. PURPOSE 4
3. POLICY DETAILS: 4
3.1 E-mailing sensitive information (including personal information) 5
3.2 General right of access to corporate e-mail 6
3.3 Staff access to e-mail services 6
3.4 Privacy and Access 6
3.5 Acceptable and Unacceptable Use of E-mail Services 7
3.6 Personal Mailbox 8
3.7 Shared Mailboxes 8
3.8 Guidelines 8
3.9 Retention of Emails 9
4. TRAINING AND SUPPORT 9
5. PROCESS FOR MONITORING COMPLIANCE 10
6. REFERENCES: 10
7. ASSOCIATED DOCUMENTATION: 11
8. DUTIES (ROLES & RESPONSIBILITIES): 12
8.1 Chief Executive / Trust Board Responsibilities: 12
8.2 Executive Director of Finance & Strategy (Joint Director of IM&T and Estates): 12
8.3 Senior Information Risk Owner (SIRO) Responsibilities: 12
8.4 Caldicott Guardian Responsibilities: 13
8.5 Business Managers' Responsibilities: 13
8.6 Joint Information Governance Board Responsibilities: 13
8.7 Trust Information Security Managers' Responsibilities 13
8.8 Information Asset Owners/Administrators 14
8.9 Staff Responsibilities: 15
8.10 Approving Committee Responsibilities: Joint Information Governance Board 15
9. ABBREVIATIONS / DEFINITION OF TERMS USED 15
DOCUMENT CONTROL 17
APPENDIX 1: GUIDE TO USING EMAIL 19
APPENDIX 2: GUIDANCE ON WHAT CONSTITUTES A RECORD OF VALUE 21

1. INTRODUCTION

This Policy supports the Trusts in complying with information legislation that applies to e-mail use, including the General Data Protection Regulations, Data Protection Act 2018, Freedom of Information Act 2000 and Regulation of Investigatory Powers Act 2000. In addition to complying with legislation, both Trusts will ensure that appropriate business records are maintained for audit and accountability purposes. Management of e-mail will be undertaken in such a way that staff are treated with respect and that their rights are not violated.

2. PURPOSE

The purpose of this document is to jointly define the policy for the use of e-mail within North Cumbria University Hospitals NHS Trust and Cumbria Partnership NHS Foundation Trust.

The objectives of this policy are:

- To ensure that the Trusts comply with their legal obligations.
- To promote the use of email to support the clinical and operational work of the Trusts.
- To ensure that Trusts' IT resources are not misused.
- To ensure that the security of computer systems and the information they contain is not compromised in any way.
- To prevent the Trusts' reputations from being damaged by the inappropriate or improper use of its information resources.

3. POLICY DETAILS:

Email is the main business tool for both internal and external communication and as a result must be treated with the same level of attention given to drafting and managing formal letters and memos. Failure to do so risks legal action against the Trust and/or its employees.

Email messages must not be treated as an extension of the spoken word because their written nature means they are treated with greater authority. As well as taking care over how email messages are written it is necessary to manage email messages appropriately after they have been sent or received.

All email messages are subject to Data Protection and Freedom of Information Legislation and can also form part of the corporate record. Staff must also be aware that email messages could be used as evidence in legal proceedings.

A record can be defined as information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

E-mails may typically be considered as records if the message:

- Clearly concerns official business;
- Requests a reply or action and is about business matters;
- Contains a decision about business matters;
- Is an external e-mail, to or from another business entity.

For further information on what constitutes a 'record of value' please go to Appendix 2.

3.1 E-mailing sensitive information (including personal information)

There are two broad areas of sensitive information that could be potentially communicated via e-mail – information considered commercial in confidence, and personal information. It is important that these types of information are communicated with care, because if they are communicated to the wrong people it could result in the Trust or members of staff being involved in legal action.

Under GDPR sensitive data is now classified as "special categories of personal data" additionally it carries the following constraint, "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life of sexual orientation shall be prohibited".

The privacy and confidentiality of the messages sent via e-mail cannot be guaranteed. It is the responsibility of all members of staff to exercise their judgement about the appropriateness of using e-mail when dealing with sensitive subjects. Staff members are advised that putting disclaimers on external e-mail does not guarantee protection for individuals from potential legal action if e-mails sent include unsupported allegations, sensitive or inappropriate information.

Staff must ensure that all information of a sensitive nature that is sent via e-mail is treated with care in terms of drafting and addressing.

E-mail messages containing personal information are subject to the Data Protection Act. Personal information includes opinions about an individual or the personal opinions of an individual. E-mail messages containing this type of information should only be used for the purpose for which the information was provided, be accurate and up to date, and must not be disclosed to third parties without the express permission of the individual concerned.

E-mail messages that contain information not intended for general distribution must be clearly marked either in the title or at the beginning of the message, for example an e-mail message containing comments about the performance of a specific staff member or group of staff. This should decrease the likelihood of the message being forwarded to unintended recipients. Identities must not be included in the subject line of a sensitive email.

E-mail messages that contain information that is not supported by fact must indicate that it is the sender's opinion that is being expressed.

3.2 General right of access to corporate e-mail

The Freedom of Information Act gives members of the public a general right of access to information held by the Trust, subject to specific exemptions which may apply. E-mails are just another type of record within the organisation, and as such e-mail messages may be disclosable.

3.3 Staff access to e-mail services

Cumbria Partnership NHS Foundation Trust and North Cumbria University Hospitals NHS Trust provide electronic mail services to staff to enable them to communicate effectively and efficiently with other members of staff, other Trusts and partner organisations with whom they deal in the course of their normal working duties. Electronic mail is available to all staff members.

All individual user mailboxes will be set-up by the Trusts' IT Departments upon a written request duly authorised by the requestor's Line Manager/Head of Department and should detail the business need for the service.

The services provided include:

- Microsoft Exchange accounts for internal CPFT & NCUHT users
- Maintenance of an Active Directory (AD) based Global Address List (GAL) that includes other NHS Organisations within Cumbria
- Connection via Internet/non-NHS organisations
- An electronic Personal Diary / Scheduler
- Facility to schedule meetings with other users
- Facility to create Personal Address Book(s)
- The ability to create an NHS mail (encrypted) account
- Encrypted e-mail accounts subject to approval
- Access to 7Zip encryption tools for attachments.

3.4 Privacy and Access

Although Trust e-mail messages are not personal and private, the system administrators will not routinely monitor individual staff member's e-mail and will take reasonable precautions to protect the privacy of e-mail.

Members of staff are advised that the content of email messages will be monitored if they are suspected of misusing e-mail or of excessive personal use.

Any member of staff who has the content of their email messages monitored will normally be informed before the monitoring takes place. If no further action is to be taken as a result of monitoring the content of e-mail messages then all the data collected as a result of the monitoring will be destroyed immediately.

However, only the SIRO or the Head of IG may authorise access to an employee's e-mail:

- for a legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time)
- to diagnose and resolve technical problems involving system hardware, software, or communications; and/or
- to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation within the Trust's Disciplinary Policies, or where required by the Police or other body duly authorised in law.

A staff member is prohibited from accessing another user's e-mail without his or her permission except in the above circumstances.

3.5 Acceptable and Unacceptable Use of E-mail Services

WARNING: Under no circumstances should an attachment be opened, or a hyperlink selected, if the email is not expected or comes from an unrecognised address. Also, if the email is an invitation remember also to delete it from your calendar. Users are to seek advice from the IT Service Desk.

Acceptable use of the service covers business use and work related training or research. It should be noted that, sending confidential or patient related information must be restricted to addressees currently using the North Cumbria Community of Interest Network known as the 'private circuit'. This includes addresses for this Trust and other Trusts within our local healthcare community. Emails containing sensitive information going to external addresses must be encrypted in accordance with the current NHS Standard for encryption.

The confidentiality of e-mail cannot be assured, and any confidentiality may be compromised by unintended redistribution. Users, therefore, should exercise extreme caution in using e-mail to communicate confidential or sensitive matters, and should not assume that their e-mail is private or confidential.

Personal use will only be allowed in exceptional circumstances and then only with the authority of the user's supervisor/line manager, and providing that it does not:

- Interfere with work commitments
- Constitute misuse of the email system as detailed below.

Unacceptable use of the service includes sending confidential or patient related information to external mail addresses UNLESS it is encrypted in accordance with the current NHS Standard for encryption. This also applies to redirecting email from an individual employee's North Cumbria University Hospitals NHS Trust account to their own personal home account. It also includes:

- Gambling
- Conducting illegal activities
- Non-Healthcare profit making activity (e.g. buying or selling goods or services)
- Financial transactions
- SPAM (sending unsolicited e-mail)
- Forwarding chain mail.

Staff members are forbidden to include any of the following in e-mail messages:

- Profanity
- Libellous or defamatory material
- Indecent or obscene material
- Abusive or menacing material that is likely to cause offence
- Material that is designed or likely to cause annoyance, inconvenience or needless anxiety
- Material that harasses any other employee or third party on the basis of sex, race or disability
- Material that denigrates any other employee or third party on the basis of sex, race or disability
- Material that infringes the copyright of another person
- Unsolicited commercial or advertising material.

Any behaviour or comments that are not permitted in the spoken or paper environment are also not permitted in e-mail messages.

An e-mail has the same standing in law as any other document and if the content is considered to be defamatory, it may leave both the Trust and the individual employee open to legal action.

3.6 Personal Mailbox

Users are not to use personal mailboxes for filing. Any email that is to be retained is to be saved as a file in an appropriate folder in either SharePoint or in My Documents if it is not appropriate to share. Emails should be deleted when they are no longer required.

3.7 Shared Mailboxes

Shared mailboxes should be used where there are a group of people responsible for the same area of work. Access to a shared mailbox is initially given by the IT Department and can be granted by the person who owns the mailbox.

A shared mailbox can be a way of ensuring that queries are answered quickly when members of the team are away from the office and can identify emails that should be retained as a record of an activity and delete short-lived messages.

The owner of the shared mailbox must establish a procedure for message handling for the mailbox such as how to delete an email message from the mailbox and how to identify an email message as having been answered. It is the responsibility of the owner to ensure that there are specific rules relating to the management of shared mailboxes and it is the responsibility of all staff members with access to shared mailboxes to abide by those rules. As with personal mailboxes a shared mailbox is not to be used for filing.

3.8 Guidelines

Detailed advice on how to determine and implement an appropriate level of security is available at Appendix 1.

3.9 Retention of Emails

Trust employees are responsible for managing their email records in the same way that they are responsible for managing other Trust records. Each member of staff may have a set mailbox quota for storage of emails dependent on Trust. If you exceed the maximum quota for your mailbox you will be unable to send or receive emails and will need to manage your mailbox accordingly.

It is tempting to assume that because an email provides a receipt of correspondence that the Trust should keep them all. In practice this is not a financially viable option, provides a significant burden to the Trust, creates inefficiency and increases the risk of non-compliance. In reality only a proportion of emails will contain information of value or importance to the business. Each individual is responsible for making a judgement call in identifying which emails are of value and moving these to the respective storage system you have in your department to retain as part of the official Trust record e.g. health record, electronic patient record, complaint file or similar.

How long an email should be retained is governed by the information contained within it, not the medium on which it is stored. The Trusts follow the NHS Retention Schedules which set out the classes of information held along with the recommended period for which they should be kept. Each individual is responsible for ensuring that the email is stored with other information in the system used within your department, e.g. SharePoint, health record, complaint file, or similar.

Employees must not set up a parallel filing structure for those emails constituting a record. They must be stored on the appropriate departmental shared area. Staff members should follow the Joint Corporate Records Policy & Procedure, Appendix 2 – Filing Structures.

Do not use .pst files (outlook personal folders) to archive emails. If they are stored on the local hard drive they may be lost or overlooked if they are requested under the Freedom of Information Act.

You should set your deleted item folder to empty itself on closure of the Outlook application. Deleted items should not be used as a file store. Emails deleted from your Deleted Items folder will be stored for 60 days after deletion in case they need to be recovered. After this period they will be permanently deleted.

4. TRAINING AND SUPPORT

In order to ensure the correct implementation of this policy all managers are required to ensure that all their staff are aware and have understood its content as part of approval of registration applications. Managers through Training Needs Assessments and through the outcome of investigations will identify the need for e-mail training. The IT Training Department has a full MS Office, including MS Outlook. Check with your line manager for details.

The following additional training requirements are specific to this policy:

- Employee Induction
- Mandatory Data Security Awareness training using the Trust TNA eLearning programme option: 261 – 0000 Data Security Awareness Level 1

5. PROCESS FOR MONITORING COMPLIANCE

The process for monitoring compliance with the effectiveness of this policy is as follows:

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
Email usage and filtering reports	Automated reports from the email perimeter security system showing total throughput, malware and exceptions.	Cyber Security	JIGB	Quarterly
Investigation reports	Reports on email based investigations. It should be noted that no sensitive detail is shared with JIGB.	Cyber Security	JIGB	Quarterly or as required
Compliance and knowledge checks	Report of outcomes from monthly spot checks within localities.	Head of IG	JIGB	Monthly
Access to 3rd party email accounts	Report on requests and decision for access	Head of IG	JIGB	Annually

Wherever the above monitoring has identified deficiencies, the following must be in place:

- Action plan
- Progress of action plan monitored by the Joint Information Governance Board minutes
- Risks will be considered for inclusion in the appropriate risk registers

6. REFERENCES:

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents

Regulation of Investigatory Powers Act 2000 (RIPA)
http://www.legislation.gov.uk/ukpga/2000/23/contents

Employment Practices Code
http://ico.gov.uk/for_organisations/topic_specific_guides/employment.aspx

Obscene Publications Act 1964
http://www.legislation.gov.uk/ukpga/1964/74/contents

Telecommunications Act 1984
http://www.legislation.gov.uk/ukpga/1984/12/contents

Protection of Children Act 1999
http://www.legislation.gov.uk/ukpga/1999/14/contents

Copyright, Design and Patents Act 1988
http://www.legislation.gov.uk/ukpga/1988/48/contents

Equality Act 2010
http://www.legislation.gov.uk/ukpga/2010/15/contents

Computer Misuse Act 1990
http://www.legislation.gov.uk/ukpga/1990/18/contents

Public Records Act 1958
http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51/contents

N.B. (This is not a comprehensive list of the law that could be relevant.)

7. ASSOCIATED DOCUMENTATION:

Information on the topics listed below can be found on individual Trust Intranet pages. Direct hyperlinks have been removed due to accessibility issues during the integration. If in doubt please contact the relevant IT Service Desk or IG Officers.

CPFT Intranet: http://cptportal.cumbria.nhs.uk/Pages/Home.aspx
NCUHT Intranet: http://nww.staffweb.cumbria.nhs.uk/index.aspx

- Joint Corporate Records Policy & Procedure
- Information and Cyber Security Guidance
- Information and Cyber Security Policy
- Information Security Acceptable Use Policy
- Information Risk Policy
- Disciplinary Procedure

- Policy for the Use of Social Networking Sites.
- Email Use Guidelines
- Mailbox Management
- Email Relationship Matrix

8. DUTIES (ROLES & RESPONSIBILITIES):

8.1 Chief Executive / Trust Board Responsibilities:

The Chief Executive and Trust Board jointly have overall responsibility for the strategic and operational management of the Trusts, including ensuring that Trusts' policies comply with all legal, statutory and good practice requirements.

8.2 Executive Director of Finance & Strategy (Joint Director of IM&T and Estates):

The Executive Director of Finance & Strategy is responsible for ensuring the development and sign off of this Policy. They ensure the policy is kept up to date by the relevant author and approved at the appropriate committee.

8.3 Senior Information Risk Owner (SIRO) Responsibilities:

The SIRO has responsibility for ensuring that a Mobile Computing & Remote Access Policy is in place, and for assuring the Joint Trust Board of compliance with relevant legislative and mandated requirements. The SIRO has overall responsibility to ensure an Information & Cyber Security Policy framework is in place, including processes to monitor such use, thereby providing assurance that management of threats to security is in place, and that all employees are aware of their responsibilities

The role of the SIRO:

- Is accountable for approving all Information Assets.
- Fosters a culture for protecting and using data.
- Provides a focal point for managing information risk and incidents.
- Is concerned with the management of all information assets.
- To provide a focal point for the resolution and/or discussion of information risk issue.
- Ensure that all care systems information assets have an assigned Information Asset Owner.
- Ensuring the Organisation has a plan to achieve and monitor the right Information Governance culture, across the organisation and with its business partners.
- Approval of all information asset business continuity plans.
- Document a plan for information security assurance that identifies the support necessary to ensure work related to information security management is appropriately carried out.

- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- Review and agree action in respect of identified information risks.

8.4 Caldicott Guardian Responsibilities:

The Caldicott Guardian is appointed by the Trust Board and registered with NHS Digital. They ensure that the Trust achieves the highest standards for handling patient information. They represent and champion patient confidentiality issues within the Trust's overall Information Governance Framework

8.5 Business Managers' Responsibilities:

Business Managers must ensure that they have agreed and implemented the departmental arrangements for ensuring compliance with this policy and all policies that are related.

Managers are responsible also for ensuring adequate dissemination and implementation of Policies relevant to the staff in their areas. Managers must ensure staff can access the hard copy policy summary file on their ward / department and ensure staff members understand how to access policies on the Intranet.

8.6 Joint Information Governance Board Responsibilities:

The Joint Information Governance Board (JIGB) is responsible for reviewing this Policy, ensuring it is fit for purpose and that it is ratified and passed for publication. The Chair of the JIGB will ensure the policy approval is documented in the final section of the Checklist for Policy Changes. The committee will agree the approval of the final draft of the policy.

The Head of Information Governance reviews Information Governance incidents reported through the Trusts' Risk Management systems with this Policy in mind. The Head of Information Governance reports Serious IG Incidents to the JIGB. To further support the tenets of this Policy the Head of Information Governance reviews the Trusts' Information Flow Mapping on an annual basis, and reports any 'high risk' flows to the JIGB.

8.7 Trust Information Security Managers' Responsibilities

The Trust Information Security Managers are responsible for:

- Acting as a central point of contact on information & cyber security within the organisations, for both staff and external organisations.
- Implementing an effective framework for the management of security.
- The formulation, provision and maintenance of Information & Cyber Security Policies.

- Advising on the content and implementation of the Information & Cyber Security Programme.
- Producing organisational standards, procedures and guidance on Information & Cyber Security matters for review by the Caldicott Guardians and other senior staff represented on the JIGB, and other Governance Committees, on behalf of the Joint Trust Board,.
- Co-ordinating information & cyber security activities particularly those related to shared information systems or IT infrastructures.
- Liaising with external organisations on information & cyber security matters, including representing the organisations in cross-community issues.
- Ensuring that contingency plans and disaster recovery plans are reviewed and tested on a regular basis.
- Representing the organisations on internal and external bodies that relate to security.
- Ensuring the system, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally.
- Approving System Level Security Policies (SLSP) for the infrastructure and common services.
- Providing an incident and alert reporting system.
- Maintain contact with special Interest Groups in order to:

    - Keep abreast of “best practice”.
    - Maintain current knowledge of security-related matters.
    - Receive early warnings, alerts, advisories, etc. pertaining to developing threats[1].
    - Gain access to specialist advice.
    - Share and exchange information about new technologies, new threats, products, vulnerabilities, etc.

- Providing advice and guidance to Information Governance and users where applicable on:

    - Policy Compliance
    - Incident Investigation
    - Security Awareness
    - Security Training
    - Systems Accreditation
    - Security of External Service Provision

8.8 Information Asset Owners/Administrators

Systems and procedures must be put in place for each asset for which they are responsible thus enabling all employees to co-operate in the achievement of these objectives, including business contingency plans in the event of system unavailability.

[1] Such as the NHS Digital CareCERT Information sharing Portal
https://nww.carecertisp.digital.nhs.uk/display/CC/CareCERT+Information+Sharing+Portal+Home

IAOs must also ensure that email use is managed when used in conjunction with systems for which they are responsible.

8.9 Staff Responsibilities:

All staff members are responsible for reading and co-operating with the contents of this Policy as part of their normal duties and responsibilities. They are responsible for ensuring that they maintain up to date awareness of Information Security practices with regard to their own and their staff roles and responsibilities. This includes the responsibility to report information security incidents as soon as they occur.

8.10 Approving Committee Responsibilities: Joint Information Governance Board

The Joint IG Board is the oversight committee for all items relating to information governance and reports into the Joint Clinical Governance Group and Quality and Safety Committee (Board Sub Committees) as required. In terms of policy responsibilities the role of the Joint IG Board is to ensure that local policies compliment the national policy, strategy and guidance relating to information governance and that it is implemented and evaluated appropriately within the Trust. The Joint IG Board are responsible that regular review of information governance policies and procedures takes place and monitors policy compliance at each of its meetings.

The Joint Information Governance Board (JIGB) is responsible for reviewing this Policy, ensuring it is fit for purpose and that it is ratified and passed for publication. The Chair of the JIGB will ensure the policy approval is documented in the final section of the Checklist for Policy Changes. The committee will agree the approval of the final draft of the policy.

The Head of Information Governance reviews Information Governance incidents reported through the Trusts' Risk Management systems with this Policy in mind. The Head of Information Governance reports Serious IG Incidents to the JIGB. To further support the tenets of this Policy the Head of Information Governance reviews the Trusts' Information Flow Mapping on an annual basis, and reports any 'high risk' flows to the JIGB.

9. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
AD	Active Directory
AUP	Acceptable Use Policy
DLP	Data Loss Prevention
GAL	Global Address List
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
ICT	Information Communications Technology
IG	Information Governance

IGG	Information Governance Group
IM&T	Information Management & Technology
ISMS	Information Security Management System
MS	Microsoft
N3	NHS National Backbone Network
PID	Patient/Personally Identifiable Data
SIRO	Senior Information Risk Owner
UPS	Uninterruptable Power Supply
USB	Universal Serial Bus
VPN	Virtual Private Network
WAP	Wireless Access Point

TERM USED	DEFINITION
Attachment	A computer file sent along with an email message. One or more files can be attached to any email message (e.g. data files, spreadsheets, pictures etc.).
Electronic Mail	Commonly called email, is a method of exchanging digital messages from an author to one or more recipients.
Hyperlink	Contained within the email it is normally blue in colour and underlined, it is activated when selected (looks like this).
Malware	Software intended to do damage, deny access to disable computers and computer systems
Recipient(s)	The person or persons to whom the email was sent and for whom it was intended.
Sender	The person sending the email. For the purposes of this document this also refers to the author of the email.
Social Media	Websites and applications that enable people to create and share content thereby participating in electronic social interaction

DOCUMENT CONTROL

Equality Impact Assessment Date	
Sub-Committee & Approval Date	Joint Information Governance Board 15/03/2019

History of previous published versions of this document: separate CPFT/NCUH policies

Version	Ratified Date	Review Date	Date Published
NCUH IG11 Email V5.0	17/11/2016	Oct 2019	17/11/2016
CPFT Email POL/002/004 VFeb16	10/2/2016	Mar 2019	Feb 2016

Statement of changes made from previous version

Version	Date	Section & Description of change
0.1 Draft	March 2018	• Joint policy drafted in new template
0.2 Draft	September 2018	• Moved content to new joint template • Amended Executive Director to title not incumbent • Added comments in 3.1 to include GDPR and definitions • Revised Responsibilities • Amended Associated Documentation to reflect current difficulties in accessing both Intranets • Added stakeholder list • Added Appendix on 'Records of Value' • Added stakeholder amendment to remind users not to set up parallel filing structures for emails of record per the Joint Corporate Records Policy
0.3 draft	12/03/2019	• Reference to previous trust policies in Doc Control section
0.4 draft	19/03/2019	**Amended following Policy Management Group meeting:** • Added Joint IG Board approval date to Policy front page and document control section, and Policy Checklist • Section 8.5 Joint IG Board Responsibilities added clarification that this is the approving committee for the Policy. • Section 8.3 Removed Associate Medical Director and left as Caldicott Guardian • Added SIRO responsibilities

List of Stakeholders who have reviewed the document

Name	Job Title	Date
Michael Smillie	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)/Senior Information Risk Owner	04/09/2018
Robin Andrews	Interim Executive Director of Finance	04/09/2018
Andrew Brittlebank	Medical Director	04/09/2018
Graham Putnam	Associate Medical Director/Chief Clinical Information Officer	04/09/2018
Dave Dagnan	Consultant Clinical Psychologist	04/09/2018
Farouq Din	Associate Director of Digital Health	04/09/2018
Daniel Scheffer	Associate Director for Corporate Governance/Company Secretary	04/09/2018
Lesley Paterson	Associate Director of Quality & Nursing (Specialist Services)	04/09/2018
Lyn Moore	Associate Director of Operations	04/09/2018
Mandy Annis	Employment Services Bureau Manager	04/09/2018
Julie Thompson	Head of Workforce Services	04/09/2018
Elizabeth Klein	Head of Nursing - Clinical Standards	04/09/2018
Jacky Stockdale	Joint Business Manager - Corporate Services	04/09/2018
Paula McBride	Deputy Business Manager	04/09/2018
Kirsty Jay	Deputy Business Manager	04/09/2018
Laura Parkinson	Head of PMO	04/09/2018
Yvonne Salkeld	Head of IG	04/09/2018
Steve Johnstone	Joint Interim Head of IT	04/09/2018
Alan Lillie	CoIN Strategic Lead	04/09/2018
Natalie Karam	Head of Performance	04/09/2018
David Franklin	Financial Systems Manager	04/09/2018
Kath Watts	Network Manager - First Step	04/09/2018
Katherine McGleenan	Clinical Quality Manager	04/09/2018
Anne Gadsden	Information Governance Officer	04/09/2018
Paul Corrie	Information Governance Compliance Manager	04/09/2018
All NCUH Business Managers		04/09/2018

APPENDIX 1: GUIDE TO USING EMAIL

Subject Line

- Ensure the subject line gives a clear indication of the content of the message
- Indicate if the subject matter is sensitive
- Use flags to indicate whether the message is of high or low importance and the speed with which an action is required
- Indicate whether an action is required or whether the email is for information only

Subject and Tone

- Greet people by name at the beginning of an email message
- Identify yourself at the beginning of the message when contacting someone for the first time
- Ensure that the purpose and content of the email message is clearly explained
- Include a signature with your own contact details
- Ensure that the email is polite and courteous
- Tone of an email should match the intended outcome
- Make a clear distinction between fact and opinion
- Proof read messages before they are sent to check for errors
- Try to limit email messages to one subject per message
- Include the original email message when sending a reply to provide a context
- Where the subject of a string of email messages has significantly changed, start a new email message, copying relevant sections from the previous string of email messages
- Ensure email messages are not unnecessarily long
- Ensure that attachments are not just longer version of emails
- Summarise the content of attachments in the main body of the mail message

Structure and Grammar

- Use plain English
- Check the spelling within the email message before sending
- Use paragraphs to structure information
- Put important information at the beginning of the email message
- Avoid using abbreviations
- Avoid using CAPITALS as this can be construed as shouting
- Try not to over use **bold** text
- Do not use emotion
- Do not send email with very large attachments **(10Mb+)**
- Do not send emails to multiple users with attachments. Save attachment in a shared area and send a hyperlink

Addressing

- Distribute email messages only to the people who need to know the information
- Use the ‘To’ field for people who are required to take further action and the ‘cc’ field for people who are included for information only

- Think carefully about who should be included in the ‘cc’ field
- Ensure the email message is correctly addressed and review all recipients.

General

- Be aware that different computer systems will affect the layout of an email message
- Avoid sending email messages in HTML format as if an email recipient is using an email system that does not allow HTML the layout will be affected
- Be aware that some computer systems might have difficulties with attachments
- Observe the restrictions on attachment size
- Try not to forward messages unnecessarily. Save a message and provide a shortcut link
- Internal emails should use pointers to attachments and not be included in the body of the text
- When absent from work the Out of Office facility must be activated

Suspicious Email

Any emails that are unexpected and look suspicious are to be immediately deleted and the deleted items folder emptied. You can also forward the email to the Suspect-Emails@ncumbria.nhs.uk. This is not a continuously monitored mailbox so if advice on the legitimacy of the mail is required contact the service desk (do not forward the email).

Receiving Encrypted Email

Some organisations will send users encrypted email that initially may confuse the recipient. These are services that are paid for by the sending organisation. If legitimate email the recipient will need to create an account with a username and password in order to access the email content, this is free. If at all unsure attempt to contact the sending organisation but do not use any contact details in the original email.

Values

In accordance with our Trust values and standards, any comments not permitted in the spoken or paper environment are not permitted in email; any comments of a derogatory nature are prohibited.

APPENDIX 2: GUIDANCE ON WHAT CONSTITUTES A RECORD OF VALUE

It is tempting to assume that because email provides a receipt of correspondence (particularly when used to transmit an attachment) you should keep them all. In practice only a percentage of emails will contain information of value or importance to the Trust and therefore need to be kept. Keeping emails does result in a significant storage burden to the Trust, creates inefficiency and increases the risk of non-compliance. Therefore it is important as part of the email policy for all staff to identify which emails are of value and locating them with other relevant information the Trust can be confident that they are retained only as long as they are required.

Understanding the value of your email information – what must be kept

Information that needs to be kept by Law - Certain pieces of legislation set out the types of information that should be kept and how long they should be kept for, for example, the Health and Safety at Work Act. Each Information Asset Owner (using the management hierarchy in place within the Trust's structure, i.e. Head of Service) is responsible for identifying within their area of responsibility on detailing the appropriate and relevant legislative record keeping requirements. The Corporate Records Group and the Health Records Departments will be available to advise on this matter. Each Head of Service will be able to advise on any specifics unique to the department's purpose.

Information that has ongoing business value - Information of business value is that which is needed to carry out business functions or to provide evidence of a business activity. Each Head of Service will be able to advise on any specifics unique to the department's purpose.

Information that has re-use value - It is important to consider whether the information might have value from a re-use perspective. Examples include -published datasets / innovative ways to create new digital applications (Apps).

Information that is of historic value – This may be, for example, significant policy documents, records of significant decisions, documents about notable events, persons or public issues. Examples include Trust Board paperwork, policy documentation, serious untoward incidents, lessons from which an organisation has learned.

All emails of value should be stored in the respective record storage facility, i.e. SharePoint and 'S' drives, and not retained in Outlook. Outlook must not be used as a storage system. Individuals must delete all emails that you do not need, i.e. for information purposes only, and don't represent a business value. All individuals are responsible for making decisions on what email is of value in line with departmental processes.