`

NHS
Leeds
Clinical Commissioning Group

EMAIL POLICY

Version:	1.1
Ratified by:	Quality and Performance Committee
Date ratified:	13/03/2019
Name & Title of originator/author:	Karen Rowe, Information Governance Manager
Name of responsible committee/individual:	Information Governance Committee
Date issued:	19/03/2019
Review date:	March 2021
Target audience:	All staff

Executive Summary
This policy has been developed to meet legal requirements and good practice around electronic communications and to reduce the potential liabilities for misuse.

In order to ensure employees are clear about their responsibilities, this policy sets out the principles to be followed at all times when employees are using electronic communications.

The development of the CCG's information and communication infrastructure involves increasing use of electronic mail (email) and internet facilities. The expectation and requirement is that employees will use these facilities in a responsible manner and for work related purposes, according to the principles set out below.

Inappropriate use of email may result in disciplinary action being taken in line with the organisation's policies.

In order to ensure compliance with CCG policies and to investigate or detect unauthorised use of the facilities the CCG will when required:

- Monitor email using all available techniques
- Investigate any cases of apparent misuse
- Make the deliberate misuse of electronic communications subject to action under our code of conduct policies.

This policy should be read in conjunction with the following

- Confidentiality and Data Protection policy
- Internet and Social Media policy

Equality Statement
This policy applies to all employees of NHS Leeds Clinical Commissioning Group and governing body members irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1. Introduction 4
2. Scope and Objectives 4
3. Accountability and Responsibilities 5
4. Risks Associated With Email 5
5. Conditions for the use of NHS mail 5
5.2 Sending Emails Containing Person, Confidential or Sensitive Data 7
5.4 Storage of Emails Containing Personal and Confidential Data 8
5.5 Email Security at Home and Out of the Office 8
6. Storage, Retention and Destruction of Emails 8
7. Managing Emails During Staff Absence 9
8. Closing Accounts 9
9. Monitoring of Email Communications 10
10. Incident Reporting 10
11. Related Law 10
11.1 Subject Access Requests 10
11.2 Common Law Duty of Confidentiality 11
11.4 Human Rights Act 1998 11
11.5 Privacy and Electronic Communications Regulations 2003 11
11.6 Computer Misuse Act 1990 12
11.7 Copyright, Designs and Patient's Act 1998 (as amended by the Copyright Computer Programs Regulations 1992) 12
12. Training 12
13. Implementation and Dissemination 12
14. Monitoring Compliance and Effectiveness of the Policy 12
15. Associated Documents 12
Other Related Documents 13
Appendix A: Email Etiquette 14

1. Introduction

NHS Leeds Clinical Commissioning Group (CCG) recognises that the use of email is a popular and important method of both internal and external communication and its use is of great benefit to the operation of the organisation. There are, however, risks associated with the use of email relating to security, confidentiality and content.

The policy set out the parameters for correct email usage and aims to ensure any potential risks are addressed.

2. Scope and Objectives

Electronic forms of communication such as email, internet and social media are now in standard use across the CCG. This improves the ability to communicate and access information, but the potential for misuse means effective methods are required to monitor such communications with a view to minimising potential misuse and to monitor for legal liabilities.

This policy has been developed to:

- Ensure employees understand their obligations and responsibilities with regard to the use of email.
- Ensure employees understand how certain legislation, such as the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018, places obligations on the CCG and their employees as to how information held by the CCG can be used.
- Reduce the potential liabilities arising from misuse. As an employer, the CCG is liable for an employee's actions if committed "in the course of employment". This can apply, even if the CCG has directly banned the acts in question, under the principles of vicarious liability. The employee may also be personally liable;
- Promote good practice and improve safety;
- Ensure employees are working in accordance with the NHS Mail Acceptable Use Policy
- Ensure all employees are aware that the monitoring arrangements used are solely for the purpose of minimising potential misuse and monitoring legal liability.

In order to ensure employees are clear about their responsibilities when using electronic communications, this policy sets out the principles to be followed at all times.

This policy must be followed by all staff who work for or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, Board members, students and any contracted staff working for the CCG.
The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

The policy applies to all email accounts that are used on CCG and non-CCG

premises including from home, internet cafes and via portable media such as Laptops, iPads and smart phones. The policy also governs personal email accounts accessed from CCG systems.

3. Accountability and Responsibilities

All employees are personally responsible for compliance with the law in relation to their use of email that involves the use of work derived information.

All Managers are responsible for ensuring that the staff they manage are aware of this policy and of their individual responsibilities in respect of this policy.

All staff are responsible for reporting information incidents and near misses including breaches of this policy, to their manager and via CCG's incident management system (Datix).

4. Risks Associated With Email

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal and non-legal risks of email which include:

- If you click a link that inadvertently opens the CCG network to cybercrime.
- If you send or forward emails with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions, you and the CCG can be held liable.
- If you unlawfully forward confidential information, you and the CCG can be held liable.
- If you send an attachment that contains a virus, you and the CCG can be held liable
- Emails can be legally binding and an individual could inadvertently enter the organisation in to a legal arrangement such as a contract.

By following the principles in this policy, the email user can minimise the legal risks involved in the use of email. If any user disregards the rules set out in this Email Policy, the user will be fully liable and may be subject to disciplinary action by the CCG.

Employees need to be aware of legal requirements for both work, and for personal use (where it may have an impact on the CCGs).

5. Conditions for the use of NHS mail

CCG staff should have a national NHS mail account. Some staff may have other accounts such as a local government email account.

The email system used by the CCG is meant for business use. The CCG's Internet and Social Media Policy together with the NHS Mail Acceptable Use Policy outlines acceptable personal usage for Internet related activity such as email.

The address for NHSmail email accounts ends in @nhs.net and can be accessed from anywhere via the Internet. NHSmail is a secure email system which encrypts email content during transfer where the recipient and senders are using nhs.net email addresses.

There is a formal, documented user registration and de-registration procedure for access to the network. Forms for new user, user changes and leavers are available via the IT Service Desk. The staff member's Line Manager must approve the user application for network and email access.

5.1 Acceptable Use

Email is a useful resource and effective communication tool, however, it may not always be the best way to communicate information, as messages may be misunderstood (See appendix A: Email etiquette). All staff should be aware of the impact that the language and material they use may have upon the recipient(s). In particular, material of the following nature must not be communicated, copied or displayed:

- Offensive or potentially offensive
- Sexually explicit
- Illegal
- Discriminatory
- Defamatory
- Political propaganda

E-mail users must not use NHSmail e-mail services to, for, or in connection with:

- Any attempt to use any aspect of the service for private/personal gain or advertising;
- Sending work related information to your personal email account
- Routing of external communications in a manner that deliberately attempts to bypass any system logging or audit functionality;
- Attempts to disguise themselves or their sending address when they use the service in order to misrepresent any aspect of a communication;
- Use of the service to disable or overload any computer system or network or to circumvent any system intended to protect the privacy or security of another user;
- Send malicious emails or viruses, 'worms', executable files designed to disrupt the work of the CCG or email recipients;
- Use email to commit the organisation to a legally binding arrangement that is outside that individuals delegated financial limits or does not follow the organisations standing financial instructions.
- Send malicious emails or viruses, 'worms', executable files designed to disrupt the work of the CCG or email recipients;
- Forward chain mail or other frivolous material;
- Violating the laws and regulations of the United Kingdom;
- Attempts to send persistent e-mail communications to an individual or mailing list when, as a result of any complaint, a warning has been issued

that further communication are not wanted; and
- Sending defamatory material by e-mail, or sending communications which knowingly cause distress or offence to another user, or transmit any files of an obscene or pornographic nature. If, in exceptional circumstances, there is a business necessity to transmit sexually explicit images of documents for a valid clinical reason, then the user should justify and obtain the permission of the Information Governance lead or the Caldicott Guardian.

Users have a responsibility to:

- Ensure that the identity of the recipient to whom they are sending an e-mail is correct;
- Reasonably understand copyright, trademark, libel, slander and public speech control laws, so that their use of the e-mail services does not inadvertently violate any laws which might be enforceable against the CCG; and
- Ensure that, should it be necessary for Person Identifiable Data to be transferred through the NHSmail Service, the obligations detailed in the section 5.2 of this are adhered to.

The primary use of the email services used by an authorised user should be related to the business of the CCG and for the purpose which the user is employed. As such the user should not have an expectation of personal privacy in the use of the email services.

5.2 Sending Emails Containing Person, Confidential or Special Category (previously known as Sensitive) Data

Where person, confidential or special category information is to be sent via email, the content must be secure and only use an encrypted method of transfer. Email may be used to transport a small amount of data (under 20MB). The Secure File Transfer service can be used to send datasets between 20MB to 2GB.

Any communication relating to patients or staff must fully comply with the Data Protection legislation and the Caldicott standards. Staff should be able to justify the need to send the information and send no more than is absolutely necessary.

Before sending an email, the recipient's details must be verified with particularly attention paid to the organisation that the individual is based in. This can best be done by using the Address Book or Check Names function.

The email must be sent securely. Sending from NHSmail to NHSmail (i.e. between email addresses ending in @nhs.net) is secure. It is important that you check the email address of the recipient is correct all CCG staff will have an association to the CCG after their name e.g. John.smith@nhs.net (NHS LEEDS CCG)

When emailing personal, sensitive or confidential data to any other domain than nhs.net, staff must place the [secure] prefix as the first word with brackets in the email subject field. NHSmail service will assess whether encryption is needed:
If the domain to which the email is being sent is accredited, the email will be sent

securely and no further encryption is required.
If the domain is not accredited and therefore insecure, NHSmail will automatically enforce the use of the encryption tool to protect the email data.
Alternatively documents contained in the email may be password protected.

Guidance is available on the NHSmail website - Sharing Sensitive Information Guidance.

The subject header of an email communication must not contain personal or confidential data. Emails must only contain the minimum amount of identifiable information required.

5.3 Phishing and Spam Emails

Email messages are increasingly a source of viruses which often sit within attached documents. NHSmail is protected by anti-virus and anti-spam software although occasionally, as with any email service, a new virus or spam message may not be immediately detected. If you are unsure of the source of an email or attachment you should leave it unopened and inform IT services. If you receive spam messages you should forward them to spamreports@nhs.net.

You must not introduce or forward any virus or any other computer programme that may cause damage to NHS or social care computers or systems. If you are found to be deliberately responsible for introducing or forwarding a programme that causes any loss of service, NHS Digital may seek financial reparation.

5.4 Storage of Emails Containing Personal and Confidential Data

When saving emails containing personal and confidential information they must be saved in a secure location i.e. on the organisational network drives and with protection appropriate to their sensitivity. Emails containing either patient or staff identifiable information must be stored on an access restricted folder on a secure network drive, they must not be stored at any point on computer desktops or local hard drives e.g. C: Drive.

5.5 Email Security at Home and Out of the Office

Staff using work email accounts at home or within other out-of-office settings need to ensure the security of the email so that other individuals cannot access or view them. The **Information Security Policy** sets out security standards in the work environment.

6. Storage, Retention and Destruction of Emails

To manage email messages appropriately, members of staff need to identify email messages that are records of their business activities as opposed to routine email messages. For example, at the start of a project, an email may include the setting out of key points for staff to consider in setting up a new process, this could be classed as a record and needs to be saved with other documentation relating to the new process. An email confirming that you are able to attend a meeting is routine and would not need to be saved for any length of time.

It is important that email messages and their attachments which are records are moved from personal mailboxes and managed in the same way as other records.

The email system itself should not be treated as an information archive. To that end staff are not allocated unlimited email storage.

Staff need to be aware, as emails are another form of record they are subject to Records Management protocols and legislation, including Freedom of Information and Subject Access requests.

- You must never delete email (or any other type of record) if you know or suspect that it may be subject to a Freedom of Information request (i.e. leading to or documenting any aspect of the decision making process).
- Emails containing important links to projects and processes and/or including decisions should be retained.
- Emails should only be retained where there is a legal requirement to do so. Please refer to the CCG's retention schedule.

Further information about emails as records is in included in the **Records Management and Lifecycle Policy.**

7. Managing Emails During Staff Absence

Staff should make arrangements for their emails to be managed during planned absences and use the Out of Office message facility to advise who to contact in their absence.

There may be instances where it is necessary to access email correspondence from an individual's mailbox when a person is away from the office for an extended period e.g. illness or failure to make adequate arrangements for planned absences.

Where it is not possible to obtain the permission of the staff member, authorisation should be requested from the Caldicott guardian / SIRO or Data Protection Officer (DPO). The request should then be submitted to the IT Helpdesk providing justification for the access and details of the person authorising access.

Access will only be provided to a person senior to the absent member of staff and is provided for the continuation of business purposes only. Emails that are clearly personal communications must not be accessed under any circumstances.

The CCG reserves the right to inspect the content of an email, including personal emails, if there is credible reason to believe that it contains evidence of unlawful activity, including instances where there may be a breach of policy constituting gross misconduct or where there is reason to believe that it contains harmful material e.g. a file containing a virus or where the law requires it.

8. Closing Accounts

When a member of staff leaves the CCG, their Line Manager must inform IT Services that they have done so. If they have an organisational account it must be closed. The

status of the NHSmail account will be dependent what the staff member's arrangements are after they leave the CCG.

9. Monitoring of Email Communications

The use of email is covered by the NHSmail Acceptable Use Policy, and should be read in conjunction within this policy.

Line managers should monitor staff compliance with the email policy. Concerns should be raised with staff members if they are seen to not be working in accordance with the policy

All emails are monitored for viruses, however staff should be aware that these are not always automatically detected and blocked. The content of emails is not routinely monitored, however, the CCG reserves the right to retain message content as required to meet legal and statutory obligations, for example to assist with a criminal investigation.

Monitoring of content of a staff member's emails would only occur where there was a clear suspicion of criminal activity and in accordance with legislative conditions.

Access to a staff member's email may occur to ensure the continuance of business services (See Section 7) although staff must be made aware of this where this occurs.

10. Incident Reporting

All actual, potential or suspected incidents involving use of email, the internet or social media must be reported in line with the CCG's Incident Reporting Policy.

The Information Governance team will report Serious Information Governance and Cyber Security incidents to the Information Commissioner's Office. Failure to do so could result in an enforcement notice or a monetary fine. These will be usually incidents where there is a loss of personal data involving a large amount of individuals or particularly sensitive personal and confidential information has been disclosed without the legal basis to done so or in error.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity through the Report NHS Fraud website or telephoning 08000 28 40 60.

11. Related Law

This section sets out key legislation and common law affecting the use of email.

11.1 General Data Protection Regulations

Individuals have the legal right to request personal information that is held about them by organisations processing personal information; this is known as a Subject Access Request or SAR. Requests could come from individuals such as service users, complainants, and CCG staff. It could be possible that following receipt of a subject access request, that email content an employee holds and/or has produced could be subject to release as part of a request where those emails contain personal

information relating to the individual. Where such a request is received, staff may have to search through their emails and filing systems for any relevant email content for consideration of release.

11.2 Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances:

- Where the individual to whom the information relates has consented;
- Where disclosure is in the public interest (the needs of the many outweigh the confidentiality concerns of an individual); and
- Where there is a legal duty to do so, for example a court order.

Confidential information could relate to personal information of an individual or information contained in a business related document e.g. a Contract.

11.3 Freedom of Information Act 2000

Allows the right of access to anyone to recorded information held by a public authority (such as a CCG) through either a request for specific information or through accessing information via the Publication Scheme. Release of information is subject to exemptions and conditions of the Act.

Information held on a staff member's email communications may be caught by the Act if they are relevant to a specific request that has been received. In which case, the staff member would need to search for relevant email content and provide that content to the Information Governance team.

11.4 Human Rights Act 1998

Article 8 of the Act provides a right of privacy for individuals. In complying with the Act, public authorities (to which the Act applies) such as the CCG need to ensure that personal and confidential information is not disclosed unless a legal justification exists to do so.

11.5 Privacy and Electronic Communications Regulations 2003

The Regulations cover:

- Marketing by electronic means, including marketing calls, texts, emails and faxes. The Regulation specifies a clear need for consent when emailing or texting individuals (referred to as subscribers). It should be noted that the definition of 'marketing' is very broad and includes seeking to influence individual's behaviour.
- The use of cookies or similar technologies that track information about people accessing a website or other electronic service.
- Security of public electronic communications services.
- Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (e.g. caller ID and call return), and directory listings.

11.6 Computer Misuse Act 1990

Under this Act it is an offence to have unauthorised access to computer material or to undertake unauthorised modification of programs or data on a computer.

11.7 Copyright, Designs and Patient's Act 1998 (as amended by the Copyright Computer Programs Regulations 1992)

No member of staff shall infringe copyright in copyright works stored on Internet sites. Staff should note that downloading copyright text or images from an Internet site without permission may constitute infringement of copyright even if it is not the intention to republish such works. Staff must **always** check copyright notices on websites.

12. Training

All staff must undergo Information Governance training annually. All staff will receive Information Governance training via the CCG Statutory and Mandatory Training Programme. Managers must actively ensure that all staff undertake the applicable and mandatory Information Governance training.

13. Implementation and Dissemination

Following ratification by the Quality and Performance Committee this policy will be disseminated to staff via the Staff e-bulletin and communication through in-house staff briefings.

This Policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

14. Monitoring Compliance and Effectiveness of the Policy

An assessment of compliance with requirements, within the Data Security and Protection Toolkit (DSPT), will be undertaken each year. The DSPT includes requirements relating to confidentiality, data protection, security of and access to information. Incidents are reported and all serious information governance issues must be reported by the SIRO at Governing Body level and in Annual Reports.

Any breaches of this policy will be fully investigated in accordance with CCG processes which may result in disciplinary action, referral to the Local Counter Fraud Specialist for further investigation and, if appropriate, your employment or association with the CCG being terminated. It may result in disciplinary, civil or criminal proceedings.

15. Associated Documents

This policy should be read in conjunction with the Information Governance Policies:

- Information Governance Strategy
- Information Governance Policy and Management Framework
- Confidentiality and Data Protection Policy
- Freedom of Information and Environmental Information Regulations Policy

- Information Security Policy
- Network Security Policy
- Records Management and Information Life Cycle Policy
- Safe Transfer Guidelines and Procedure
- Subject Access Request Procedure

Other Related Documents

- Incident Reporting Policy
- Risk Management Strategy
- Internet and Social Media Policy
- Mobile Working Policy
- Disciplinary Policy
- Anti-Fraud, Bribery and Corruption Policy
- Whistle Blowing Policy

Appendix A: Email Etiquette

Email titles

The subject heading (or title) of your email should be relevant, clear, brief and not contain identifiers this will help you to file, retrieve and prioritise the content of the message.

Email signature format

Electronic communication is a major element of corporate identity. We send out more emails than letters and email is therefore more visible to more people than any other form of communication. A standard form of email signature has been created. Please ensure it appears at the end of all your emails and also on the out of office.

Messages supporting corporate priorities can be included on email signatures. Please first consult the communications team to ensure information is in line with current organisation-wide priorities.

- **First name Last name**
- Job title
- Department
- NHS Leeds Commissioning Group
- Address
- **Tel:** (telephone number)
- **Mob:** (mobile number if applicable)
- **Email:** xxxxxx@nhs.net

Email content

- All email message content should be written in lower case. CAPITAL letter can be considered aggressive.
- Remember to keep it short and simple - avoid sending lengthy emails with the whole history of a topic if it is possible to do so.
- Put different topics in separate emails; don't put them in one long email if you there is a lot of content consider writing a document and sending it as an attachment.
- Care should be taken in the content. Nothing should be said in an email that could not be written in a letter or spoken face to face. Staff need to be aware that emails could end up being disclosed to the public in response to a Freedom of Information / Subject Access or Environmental Information Request.
- Staff should include their name, job title, organisation title and contact details at the end of emails.
- Read receipts - when sending an email, requesting a read receipt only indicates a message was opened, not necessarily read, understood and acted upon. Read receipts should not be routinely requested as

this increases email traffic volumes. Not all systems will generate read receipts.

- Read through your email before sending it:
  - check your spelling and the layout
  - check that your content is clear and correct
- Do not count on users reading their email every day. Urgent messages like stating you cannot make a meeting are best communicated by phone in the first instance, and only sent by email as a backup.
- Only use the *High importance* level indicator on messages that warrant it.

Addressing and sending your email

- Check recipient details.
- Be selective, only send the email to those who really need it.
- Take care when addressing email to someone for the first time particularly when using NHS mail which is a national system. Do not assume that the email of the person you want to contact will be firstname.surname@..... When using NHSmail - to ensure you send the message to the correct person you can show the person's organisation next to the email address in the email address box e.g. john.smith4556734445@nhs.net (NHS LEEDS CCG). This can be done by clicking on the icon above *Check Names*

Managing your Inbox and attachments

- Process or action your emails as soon as possible
  - Consider putting a reminder to yourself by marking items *urgent* or *flagged* for follow up
  - Try not to print emails unless absolutely necessary
- As soon as emails have been actioned either file or delete them.
- Keep the number of emails in your inbox down to a minimum.
- Make sure deleted items are actually deleted by regularly emptying the *Deleted Items* folder.
- Save the attachment rather than the email.

Replying and forwarding

- Please note that attachments are automatically removed when you use *Reply* and included when you use *Forward*
- Always use the Out of Office Assistant if you are going to be away from the office
  - Give the details of anyone who is covering for you
  - Never give away personal information e.g. that you're away on holiday