Creating a healthier Hull

NHS
Hull Clinical Commissioning Group

Email Policy

2015

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

Name of Policy:	Email Policy
Date Issued:	8 March 2016
Date to be reviewed:	2 years from approval date

Policy Title:	Email Policy
Supersedes: (Please List)	Email Policy v1.0
Description of Amendment(s):	Addition of HSCIC NHSMail: Sending an encrypted email from NHSmail to a non-secure email address.
This policy will impact on:	All Staff
Financial Implications:	No change
Policy Area:	Data Protection
Version No:	1.1
Issued By:	Yorkshire and Humber CSU IG Team
Author:	Yorkshire and Humber CSU IG Team
Document Reference:	N/A
Effective Date:	8 March 2016
Review Date:	March 2018
Impact Assessment Date:	Complete

APPROVAL RECORD	Integrated Audit and Governance Committee	08 March 2016
Consultation:	Members of SLT	18 January 2016

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
1.0	Barry Jackson	Approved version		
1. 1	Helen Sanderson	Addition of HSCIC NHSMail: Sending an encrypted email from NHSmail to a non-secure email address		

CONTENTS

INTRODUCTION

1.1 Introduction

Hull Clinical Commissioning Group (from this point onwards known as the CCG) operates the national NHS Mail system as its e-mail solution for all staff. Staff must ensure that they follow the NHS Mail Policies as available with the national system as well as this local policy.

1.2 Applicability

All staff employed by CCG will have access to an NHS mail account. Contractors and temporary staff can also be granted accounts where appropriate. All CCG official business must be conducted on NHS Mail accounts. Non NHS Mail account will not be permitted in any formal Distribution Lists without the approval of the CCG SIRO.

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG etc

5 POLICY PURPOSE & AIMS

5.1 Security.

NHS Mail is a secure system operated for the NHS which is approved for the sending of patient level data. It is Government accredited to RESTRICTED status and approved for exchanging clinical information with other NHS mail and Government Secure intranet (GSi) users by the Department of Health and endorsed by the British Medical Association, Royal College of Nursing and Chartered Society of Physiotherapy. GSi domains that are secure for the exchange of patient data are: .x.gsi.gov.uk; .gsi.gov.uk; .gse.gov.uk; .gsx.gov.uk; .pnn.police.uk; .cjsm.net; .scn.gov.uk; .gcsx.gov.uk, .mod.uk.

NHSMail also includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services.

Once a message is sent from NHSmail it is encrypted and protected with a digital signature to assure the recipient that the message is authentic and has not been forged or tampered with. Formatting of the message is preserved and attachments can be included.

5.2 Virus Protection.

IMT will ensure that the appropriate technical steps are taken to reduce the vulnerability of the CCG systems to attack from computer viruses. Users are expected to play their part by being aware of the problem of viruses and reporting anything they deem to be suspicious to the IT Helpdesk. Users should note in particular to be very wary of e-mails from addresses that they do not recognise and under no circumstances should you open an attachment on an e-mail if it is not from an address you recognise and that you were expecting the attachment.

5.3 Bandwidth.

This is the term that is used to describe the amount of information that can be transmitted on a network over a given time. Individual users sending very large files such as videos or sending to large numbers of addressees can have an adverse effect on the availability of the network for other users. To avoid this, users should be aware of the problem and where possible avoid sending large e-mails with attachments. Text should be included in the body of the message as opposed to attaching a Word document, and where a file can be located on the network or Intranet the location should be given rather than copying the file. This is particularly important for multiple addressees.

5.4 Access.

Email accounts can be accessed in the following ways:

- Organisation PC or laptop using Microsoft Outlook.
- Organisation PC or laptop using Outlook Web Access.
- Non-Organisation PC or laptop using Outlook Web Access (Webmail client) through a web-browser.
- Organisation owned mobile device.

- Personal mobile devices which support appropriate security measures including non-removable 'at rest' encryption (See list in NHS Mail Guidance section for up to date information). The Organisation provides no support for personal devices connected to NHSmail.

5.5 Inappropriate Use of Email

The use of e-mail in the following types of activities is specifically prohibited.

- Illegal, fraudulent, or malicious activities.
- Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no connection with CCG.
- Unauthorised fund-raising or similar activities, whether for commercial, personal, or charitable purposes.
- Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.
- Annoying or harassing another person, e.g., by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language in an e-mail message.
- Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.
- Viewing, damaging, or deleting files or communications belonging to others without appropriate authorisation or permission.
- Attempting to circumvent or defeat security or auditing systems without prior authorisation and other than as part of legitimate system testing or security research.

These, and other inappropriate activities, may result in disciplinary action being taken against the person found misusing the e-mail service for such purposes.

5.6 Management of Email

5.6.1 There is a common misconception that email messages constitute an ephemeral form of communication. This misconception about how email messages can be used could result in legal action being taken against CCG or individuals. All email messages are subject to Data Protection and Freedom of Information Legislation and can also form part of the corporate record. Staff should also be aware that email messages could be used as evidence in legal proceedings.

5.6.2 There may be occasions when it is necessary to access email messages from an individual's mailbox when a person is away from the office for an extended period, for example holiday or sickness. Whilst users are entitled to expect a level of privacy in relation to their e-mail correspondence they must understand that this will not be an absolute right and that the needs of the organisation may override it in certain circumstances. The reasons for accessing an individual's mailbox are to action:

- Subject access request under the Data Protection Act
- Freedom of Information request
- Evidence in legal proceedings
- Evidence in a criminal investigation
- Line of business enquiry
- Evidence in support of disciplinary action

Where it is not possible to ask the permission from the member of staff whose mailbox needs to be accessed, the procedure for gaining access their mailbox is:

- Gain authorisation from Head of Department.
- Submit a request to IMT Help Desk.
- Request must be authorised in IMT by senior manager.
- A record is made of the reasons for accessing the mailbox together with the names of the people who were present.
- Inform the person whose mailbox was accessed at the earliest opportunity.

It is less likely that this procedure will need to be followed if email records are managed appropriately or mailbox access has been delegated to a trusted third party.

5.7 Records Management

5.7.1 Email messages can constitute part of the formal record of a transaction, decision or communication about an issue. All members of staff are responsible for identifying and managing emails messages that constitute a record of their work. When an email is sent or received a decision needs to be made about whether the email needs to be captured as a record. Once an email message has been captured as a record it should be deleted from the email client. The main points to consider when managing email records are:

- Identifying email records
- Who is responsible for capturing email records
- Email messages with attachments
- When to capture email records
- Where to capture email records
- Titling email records

5.7.2 Email messages with attachments. Where an email message has an attachment a decision needs to be made as to whether the email message, the attachment or both should be kept as a record. The decision on whether an email and/or its attachment constitute a record depends on the context within which they were received. It is likely that in most circumstances the attachment should be captured as a record with the email message as the email message will provide the context within which the attachment was used. There are instances where the email attachment might require further work, in which case it would be acceptable to capture the email message and the attachment together as a record and keep a copy of the attachment in another location to be worked on. In these circumstances the copy attachment that was used for further work will become a completely separate record.

5.7.3 When to capture. Email messages that can be considered to be records should be captured as soon as possible. Most email messages will form part of an email conversation string. Where an email string has formed as part of a discussion it is not necessary to capture each new part of the conversation, ie every reply, separately. There is no need to wait until the end of the conversation before

capturing the email string as several subjects might have been covered. Email strings should be captured as records at significant points during the conversation, rather than waiting to the end of the conversation because it might not be apparent when the conversation has finished.

5.7.4 Where to capture. Email messages that constitute records must be either printed to paper or saved on shared drives. Email messages captured as records should be located with other records relating to the same business activity. Personal mailboxes should not be used for long-term storage of email messages. Personal mailboxes should be used for personal information or short-term reference purposes, when these emails are no longer required they should be deleted.

5.7.5 Storage. Once captured and stored the e-mail becomes subject to the same policy for records retention as any other record. The main policy for this being HSC 1999/053 "For The Record".

5.8 Good Practice and Effective Use of Email

5.8.1 The following guidelines have been included into this policy document to provide assistance to users in the effective use of Email services.

5.8.2 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

5.8.3 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 message 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 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 longer versions of emails
- Summarise the content of attachments in the main body of the email message

5.9 Structure and Grammar

- Try to 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
- Take care when using abbreviations
- Avoid using CAPITALS
- Try not to over-use bold and coloured text

5.10 Addressing

- Distribute email message only to the people who need to know the information
- Using 'reply all' will send the reply to everyone included in the original email. Think carefully before using 'reply all' as it is unlikely that everyone included will need to know your reply.
- 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

5.11 General

- Be aware that different computer systems will affect the layout of an email message
- Avoid sending email messages in HTML format
- Be aware that some computer systems might have difficulties with attachments
- Internal emails should use pointers to attachments and information held on shared drives or the Intranet

5.12 User General Responsibilities

- It is your personal responsibility to check that you are sending email to the right recipient, as NHSmail is a national system where there may be more than one person with the same name. Always check that you have the correct email address for the person you wish to send to.
- You must ensure that it is appropriate for all recipients to access the content of any email you send. Use 'reply to all' with caution.
- Emails should be treated like any other clinical / business communication and care should be taken to ensure that content is accurate and the tone is appropriate in accordance with the Organisation Values.
- You must not send any material by email that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit or pornographic.

- If you need to transmit sexually explicit material for a valid clinical reason then you must obtain permission from the Information Governance Team. Where this is the case you must keep adequate records.
- Do not send email messages using another person's email account
- Your use of the NHS Mail system must be in accordance with the organisations Acceptable Computer Use Policy

5.13 User Legal Responsibilities

- You must not use the Organisation email service to violate any laws or regulations of the United Kingdom or other countries.
- Use of the service for illegal activity is usually grounds for immediate dismissal and any illegal activity will be reported to the police.
- Illegal activity includes, but is not limited to, sending or receiving material related to paedophilia, terrorism, incitement to racial harassment, stalking, sexual harassment or treason.
- You must not attempt to interfere with the technical components, both hardware and software, of the Organisation email service in any way.
- You must not use the Organisation email service for harassment by sending persistent emails to individuals or distribution lists.
- Do not breach copyright or licensing laws when composing or forwarding emails and email attachments.
- Email is admissible as evidence in a court of law and messages are classified as legal documents. Internal emails may also need to be disclosed under the Data Protection Act (1998), Freedom of Information Act (2000) and other legislation.

5.14 Home / Remote User Responsibilities

NHSmail may be used outside the NHS network on any computer with an internet connection. However the user is personally responsible for the information security and confidentiality of e-mail in their account and must observe the following conditions when accessing NHSmail at home or other remote locations outside the NHS:-

- Log in at the NHSmail website: www.nhs.net
- Always select the "public or shared computer" option
- Do not save confidential information on a non-Organisation device
- Only print confidential information when you are certain that you will always collect the printouts immediately and secure them
- Ensure that you are not overlooked by family members and other 3rd parties
- Do not record your password on a non-Organisation device
- Passwords must be memorised, not written down
- Log out of the NHSmail application when not in use
- Do not leave the NHSmail application logged in when unattended
- Maintain an awareness of relevant Organisation policies and procedures and observe these at all times

5.15 Passwords

Users must ensure their password is kept confidential and secure at all times. You must notify the Informatics Service desk if you become aware of any unauthorised

access to your email account or if you believe your password may have been revealed.

5.16 Generic / Departmental Email Address

Generic mailboxes should be used where there are a group of people responsible for the same area of work to ensure that queries are answered quickly when members of the team are away from the office. Requests for the setting up of generic mailboxes must come from the Service Manager and be forwarded to the Informatics Service Desk for approval and creation. Access to the generic mailbox will be setup for the designated owner and it is this person's responsibility to manage and delegate access for other staff members.

5.17 Email Forwarding

Email communication sent from the Organisation email service to any non-NHS Mail or non GSi email account is insecure. Unencrypted person-identifiable and / or sensitive information must never be sent outside the NHS N3 or .GSi public sector network, either automatically or as a result of re-direction or directly. To do so is in direct contravention of NHS and Government data security requirements, and has been a prohibited practice since February 2008. Email auto-forwarding is therefore prohibited by Information Governance rules. The Information Governance team are happy to advise on the safe transport of confidential / sensitive content to non-Organisation email accounts if required.

5.18 Email Delegation

Passwords to NHSmail must not be shared (other than where specific authorisation has been given for technical reasons). The Organisation email service allows users to delegate permissions to their own email account and calendar. Contact the Informatics Service Desk for guidance on how to delegate these permissions to others.

5.19 Personal Use

Organisation email services are established to help with the provision of health and social care and this should be the main use of the service. The Organisation allows the reasonable use of email for personal use if certain guidelines are adhered to:-

- Personal use of email must not interfere with work.
- Personal emails must also adhere to the guidelines in this policy.
- Personal emails are kept in a separate folder, named 'Private'. The emails in this folder must be managed.

5.20 Private Business Use

The use of NHSmail and other resources for private business is strictly forbidden. You must not use Organisation or NHS systems for personal commercial gain, or for the personal or commercial gain of relatives or other 3rd parties. This includes, but is not limited to marketing, advertising and selling goods or services.

5.21 Email Confidentiality and Security

NHSmail is automatically encrypted in transit, therefore any email sent from one NHSmail account to another (e.g. xxx@nhs.net to yyy@nhs.net) is secure.

NHSmail is hosted on the N3 network and as such forms part of the wider public sector Government Secure Intranet (GSi). This means that we can also be assured that email is encrypted when delivered to any of the following email domains:-

Secure email domains in Central Government:

*.gsi.gov.uk
*.gse.gov.uk
*.gsx.gov.uk

The Police National Network/Criminal Justice Services secure email domains:

*.police.uk
*.pnn.police.uk
*.scn.gov.uk
*.cjsm.net

Secure email domains in Local Government/Social Services:

*.gcsx.gov.uk

Email sent to / from NHSmail addresses and email addresses ending in the above will be secure in transit. The Government is expanding GSi coverage and access to other public sector organisations and the list above may increase.

When sending outside the GSi network, personal, sensitive and confidential information must be removed from the subject line and body text of the document and sent as an encrypted attachment.

The Information Governance team is happy to advise on the safe transport of confidential / sensitive content to non-GSi email accounts if required.

NHSMail also includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services.

Once a message is sent from NHSmail it is encrypted and protected with a digital signature to assure the recipient that the message is authentic and has not been forged or tampered with. Formatting of the message is preserved and attachments can be included.

Guidance as to how to use this facility is available in 'HSCIC: Sending an encrypted email from NHSmail to a non-secure email address' and 'Guidance for recipients of an encrypted NHSMail email . These are available at:
http://systems.hscic.gov.uk/nhsmail/secure

5.22 Organisation wide Emails

Users are limited to sending out emails to a maximum of 200 users. Access to distribution lists such as "all staff" is restricted to Directors, their PA's and certain specific post holders. This facility must be used with due care and consideration.

5.23 Policy Adherence

The Organisation does not require a signed document from email users.
All email users are responsible for ensuring that they understand and comply with the contents of this policy. Individual's use of organisation computing equipment demonstrates their consent to the terms of this policy.

6 IMPLEMENTATION

The policy will be disseminated by being made available on the intranet and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

7 TRAINING & AWARENESS

Staff will be made aware of the policy via the Intranet.

8 MONITORING & AUDIT

Staff are advised that in accordance with the Employment Practices Data Protection Code monitoring of E-mail traffic will take place subject to the following guidance:

Monitoring is required to ensure that employees do not breach any regulations (such as those on harassment) which could have a legal impact on CCG.
The Information Governance Team, on the specific authorisation of the Head of IMT, will carry out checks.
Spot checks will be done as opposed to continuous monitoring.
Traffic will be monitored as opposed to content unless there are reasons for checking specific e-mails.
E-mails that are obviously personal will not be opened without the individuals consent.
Inappropriate use of the e-mail may result in the facility being withdrawn and may constitute an offence under the NHS disciplinary code.

System Monitoring

All emails are monitored for viruses.

All email traffic (incoming and outgoing) is logged automatically. These logs are audited periodically. The content of emails are not routinely monitored. However, the Organisation

reserves the right to retain and review message content as required to meet organisational, legal and statutory obligations. Breach of this policy may have contractual consequences for members of staff and could lead to legal action being taken against individuals and / or the Organisation.

9 POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

Appendix 1

1. Equality Impact Analysis	
Policy / Project / Function:	Email Use Policy
Date of Analysis:	23/11/15
This Equality Impact Analysis was completed by: **(Name and Department)**	C Wallace - IG Manager – CSU IG Team
What are the aims and intended effects of this policy, project or function ?	This standard provides practice advice on the use of the nationally provided email system NHSmail as well as detailing expected use and etiquette within the system.
Please list any other policies that are related to or referred to as part of this analysis?	
Who does the policy, project or function affect ? Please Tick ✔	Employees ☒ Service Users ☐ Members of the Public ☐ Other (List Below) ☐

2. **Equality Impact Analysis: Screening**					
	Could this policy have a positive impact on…		Could this policy have a negative impact on…		Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact
	Yes	No	Yes	No	
Race	☐	☒	☐	☒	
Age	☐	☒	☐	☒	
Sexual Orientation	☐	☒	☐	☒	
Disabled People	☐	☒	☐	☒	
Gender	☐	☒	☐	☒	
Transgender People	☐	☒	☐	☒	
Pregnancy and Maternity	☐	☒	☐	☒	
Marital Status	☐	☒	☐	☒	
Religion and Belief	☐	☒	☐	☒	
Reasoning					
If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7					

Appendix 2

SUSTAINABILITY IMPACT ASSESSMENT

Policy / Report / Service Plan / Project Title:				
Theme (Potential impacts of the activity)	**Positive Impact**	**Negative Impact**	**No specific impact**	**What will the impact be? If the impact is negative, how can it be mitigated? (action)**
Reduce Carbon Emission from buildings by 12.5% by 2010-11 then 30% by 2020			X	
New builds and refurbishments over £2million (capital costs) comply with BREEAM Healthcare requirements.			x	
Reduce the risk of pollution and avoid any breaches in legislation.			x	
Goods and services are procured more sustainability.			x	
Reduce carbon emissions from road vehicles.			x	
Reduce water consumption by 25% by 2020.			x	
Ensure legal compliance with waste legislation.			x	
Reduce the amount of waste produced by 5% by 2010 and by 25% by 2020			x	
Increase the amount of waste being recycled to 40%.			x	
Sustainability training and communications for employees.			x	
Partnership working with local groups and organisations to support sustainable development.			x	
Financial aspects of sustainable development are considered in line with policy requirements and commitments.			x	