NHS
Bury
Clinical Commissioning Group

Email Policy

Version:	2.0
Ratified by:	NHS Bury CCG Information Governance Steering Group
Date ratified:	July 2021
Name of originator /author (s):	Greater Manchester Shared Services - IT Department; NHS Bury CCG Information Governance Team
Responsible Committee / individual:	NHS Bury CCG Information Governance Steering Group
Date issued:	October 2021
Review date:	July 2022
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Email Policy CCG.GOV.016.2.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	Greater Manchester Shared Service - IT Department; NHS Bury CCG Information Governance Team
This document should be read in conjunction with	• Information Governance Framework • Information Governance Policy • Confidentiality and Data Protection Policy • Record Management Policy • Encryption Policy • Information Governance Incident Reporting Policy
This document has been developed in consultation with	NHS Bury CCG Information Governance Steering Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place, Knowsley St Bury BL9 0SN Main Telephone Number: 0161 762 1500
Copies of this document are available from	The corporate PA office (no paper copies to be provided). Electronic Copies only CCG Website People Matters

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
0.1 = draft 1	NHS Bury CCG IM&T Steering Group	February 2014
1.1 = Policy once ratified	NHS Bury Clinical Commissioning Group	February 2014
1.2 = review	NHS Bury CCG Information Governance Team	16th July 2021
1.4 = review	NHS Bury CCG Information Governance Steering Group	October 2021
2.0 = policy once ratified	NHS Bury CCG Information Governance Steering Group	July 2021

Email Policy

Contents

Contents

1. Assurance statement

1.1 Email is an important part of the CCGs and the wider NHS Communications system. Use of the installed systems/connections is for legitimate work-related purposes only and is encouraged to improve the quality of work and productivity in patient care, research, operational matters, education and development. However, we must ensure that the increasing use of information technology maintains patient confidentiality, is not misused, and at the same time is secure and accurate.

2. Introduction

2.1 The purpose of this policy is to provide guidance to all to provide guidance to all the Clinical Commissioning Group (henceforth referred to as "the CCG") staff on permissible usage of the email system.

2.2 The aims of the policy are:

- Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service;
- establish a common set of governance and usage criteria for sending, receiving and storing emails that are to be uniformly applied throughout the CCG and its constituent businesses;
- promote awareness of and adherence to the CCG Information Governance practices;
- reduce the risk to the CCG and constituent businesses of:
  - loss of reputation
  - unauthorised or inadvertent disclosure of medical, personal or
  - confidential records
  - legal liabilities;
- provide a foundation for procedures and processes that support the working practices of the organisation.

3. Aims and Objectives

3.1 This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

3.2 For the purposes of this policy the aforementioned will be referred to as users throughout the remainder of this document.

4. Mailbox Quotas and Archiving

4.1 It is the responsibility of each user to ensure they manage their email appropriately

and routinely delete unwanted emails or routinely archive emails.

4.2 Users will not be able to send or receive emails once their quota has been reached. Please contact the GMSS IT Service Desk for any assistance or advice.

5. Duties and responsibilities

5.1 Overall accountability for policy or procedural documents across the CCG lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issue in respect of policy or procedural documents.

5.2 Overall responsibility for the email policy lies with the CCG Information Governance Team or equivalent, who has delegated responsibility.

5.3 Staff will receive instruction and direction regarding the policy from a number of sources:

- policy /strategy and procedure manuals. Data transparency and Openness
- line manager
- specific training course
- other communication methods (e.g. team brief/team meetings)
- intranet

6. Main policy

6.1 The CCG email is primarily for business use. Occasional and reasonable use of personal use is permitted, provided such use does not interfere with the performance of duties and does not conflict with the CCG policies, procedures and contract of employment.

6.2 All emails must contain an email signature that conforms to the CCG corporate guidelines and agreed template.

6.3 CCG staff will be issued with an NHSMail (nhs.net) account.

6.4 It is strictly prohibited for any user to initiate or propagate the forwarding of chain letters, junk email and/or jokes. If a user receives any such email, the user should immediately notify their line manager, the IT Service Desk (GMSS) or the CCG's Head of IT.

6.5 It is strictly prohibited for any user to promote any kind of business, or business activity, except that of the CCG or its constituent businesses.

6.6 It is strictly prohibited for any user to use the personal email accounts, such as Yahoo, Google, Hotmail and others to forward or receive work emails.

6.7 It is strictly prohibited for any user to use the email facilities for the purpose of advertising, gambling, solicitation of personal goods or services for personal gain or profit, the passing of indecent, subversive criminal data across or out from the CCG when such information may cause harm to an individual, group or the CCG or any of its

constituent businesses.

6.8 The CCG will not be held liable for any financial or material loss to any individual when using the email facilities for personal incidental use or when using personal equipment to access work email.

6.9 Staff must not use another user's email account or gain access to another user's inbox. It is however, deemed acceptable for an Executive/Senior Manager to allow delegated access of their email account to their Personal Assistant/nominated member of staff. The reason for this, is that there may be occasions when a Personal Assistant/nominated member of staff is required to send emails and receive emails on behalf of their Executive/Senior Manager (when instructed to do so). If delegated access is required, then the necessary procedure and process must be fully adhered to and the GMSS IT Service Desk contacted also.

6.10 Staff must not send global emails to ALL staff or to ALL GP practices of a personal nature. Global emails should only be used for when sending the same business email to a group of staff. There are processes that must be followed for such communications. Contact the relevant Communication Team for advice and guidance.

6.11 Staff must not use emails for political lobbying.

7. Confidentiality

7.1 Users must always comply with data protection laws and should be able to justify the need to send personal identifiable data and send no more than is absolutely necessary. Users should consult their line manager or Information Governance Manager (or equivalent) if they have any questions.

7.2 Users sending personal identifiable data, patient data, sensitive or confidential information via email must do so in a secure manner; by using an encrypted method of transfer as seen in NHSmail. Email may be used to transport a small amount (max 20MB), while a secure file transfer service can be used to send datasets that are more than 20MB. Sending email from NHSmail to NHSmail (email addresses with domain name nhs.net) is secure and does not require additional measures.

7.3 Tips:

- Person identifiable, sensitive or confidential information must not be sent unprotected to external non-nhs.net email addresses. For example firstname.lastname@nhs.net to **x.y@ACUTE.nhs.uk**. If in doubt, always ask.
- Users must not send emails to large number of users unless the recipients have been suitably "Blind Copied" (bcc). This practice will ensure email addresses are not visible to all recipients, which may compromise the confidentiality of one or more recipients and this is classed as a Data Breach.
- 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.

7.4 Users should always cross check that the recipient address is correct, all CCG staff will have the current location attached to their name e.g. **firstname.lastname@nhs.net** (NHS Bury CCG).

7.5 Some emails addresses as listed below have the same high accreditation and security standards as NHSmail.

NHS (*.nhs.net)
CJSM (*criminal justice secure mail)
PNN (*pnn.police.uk)
MoD (*.mod.uk)
SCN (*scn.gov.uk
Gov.uk, Gov.wales, Gov.scot

7.6 Since March 2019 - Below are now retired domains as advised by the cabinet office

GCSX (*.gcsx.gov.uk)
GSI (*.gsi.gov.uk)
CJSM (*cjsm.net)
GSE (*.gse.gov.uk)
GSX (*.gsx.gov.uk)

7.7 **Never put patient safety at risk.** If in doubt as to whether it is justifiable to anonymise / pseudonymise the information, speak with Line Manager or the Information Governance Team in the first instance

7.8 However, when emailing personal, sensitive or confidential data to any other domain e.g. hotmail, yahoo, gmail etc. users must place the [secure] prefix as the first word with square 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.

7.9 Alternatively, documents contained in the email may be password protected.

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

8. Implementation Process

8.1 This policy will be reviewed on an annual basis, and in accordance with the following on an as and when required basis:

- legislative changes
- good practice guidance
- case law

- significant incidents reported
- new vulnerabilities
- changes to organisational infrastructure

8.2 The CCG aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and public have been reviewed in line with the organisational legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief.

9. Monitoring Arrangements

9.1 Email usage and content is monitored for the purposes of :

- Providing evidence of communication
- ensuring adherence or compliance with the CCG business standards, policies, procedures and contractual agreements;
- ensuring compliance with legal obligations such as the Freedom of Information Act 2000 (FOIA), the Data Protection Act 2018 and UK GDPR 2021;
- monitoring standard of service, employee's performance and as a tool for employee training;
- preventing or detecting unauthorised use of the CCG communication systems
- identification, detection, quarantine and removal of malicious software or programs;
- reporting of offensive emails to management.

9.2 All emails are potentially disclosable to the public under FOIA.

9.3 If user sees or has evidence of unacceptable use, the user should report this to their line manager. If users are unable to do this, it should report the incident via the usual incident reporting procedures.

10. Legislation and related documents

10.1 <u>Associated Legislations</u>

- Copyright, Designs & Patents Act 1988
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- The Data Protection Act 2018
- The Human Rights Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Environmental Information Regulations 2004 (EIRs)
- Freedom of Information Act 2000

- Health & Social Care Act 2012

11. CCG Guidelines

11.1 The CCG considers email as an important means of communication. It recognises the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. The CCG wishes to encourage Users to adhere to the following guidelines:

- Acknowledgement for emails should be sent within a reasonable period. This is a good business practice and staff should be encouraged to follow this practice. Sometimes certain requests may come in the form of an email e.g.: a Subject Access request or a FOIA request. This should be straightaway forwarded to the relevant line manager or personnel. There is a certain time frame prescribed for these requests and delay could result in a fine for the CCG. Act promptly.
- If you are going to be away from your desk and unable to check your emails, you should use the out of office function. The out of office reply should state when you will return to the office and who to contact in your absence.
- 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 these increases email traffic volumes. Also, not all systems will generate read receipts.
- Ensure you send your email **only to people who need to see it**. Identify the correct person to receive your email. Only copy those people who really need to see the email. Do not automatically copy your email to directors or other senior members of staff.
- Write well-structured and polite emails. Always address the recipient with an appropriate greeting and end your message with a suitable sign off, such as regards or best wishes.
- State any actions required by the recipient. If you need a reply to your email by a particular date let the recipient know this.
- The content of the email and the signature must follow the corporate standard. A disclosure statement should also be included at the end of your signature. This is usually automatically added when an email is sent.
- Do not write emails in capitals. This appears as if you are shouting and is considered rude. As with all CCGs correspondence, emails should be written in Arial font size 11 (minimum) in black or blue.
- Always use the subject box, providing a short description of the subject and its urgency.
- Only mark emails as important if they really are important.
- Do not send unnecessary attachments.
- Recognising the CCG's outlook on paper-free, digital-first approach - Do not print emails unless you really need to for work purposes.
- Emails can be saved if you need them. To save emails you should create your own filing system within the personal folder in your inbox. Remember that all emails kept on the system can be recalled under the Freedom of Information Act. You should therefore only keep those emails that are necessary.

- Emails should be archived on a regular basis. For guidance please contact the IT Service Desk.
- Delete any email messages that you do not need to have a copy of.
- Never allow anyone to know or use your email user ID and password.
- Do not leave your email open and unattended – use a password protected screensaver.
- If you suspect you received a virus by email contact the IT support team immediately and do not open the email. Do not attempt to remove the virus yourself. The IT Service Desk will need to know what virus it is.
- Unsolicited commercial emails (Spam) should be deleted. High volumes of spam should be report to the IT Service Desk.
- If you suspect that you have received phishing e-mail, do not click on any links and provide any information, report to the GMSS IT Service desktop to investigate.