NHS
Barnsley
Clinical Commissioning Group

BARNSLEY CLINICAL COMMISSIONING GROUP'S EMAIL POLICY

March 2018

Version:	3.0
Approved By:	Governing Body
Date Approved:	13 February 2014 January 2016 (reviewed) March 2018 (reviewed)
Name of originator / author:	Gershon Nubour
Name of responsible committee/ individual:	Quality and Patient Safety Committee (Approval) IG Group (review)
Name of executive lead:	Richard Walker
Date issued:	July 2018
Review Date:	2 years from approval
Target Audience:	Barnsley CCG staff

THIS POLICY HAS BEEN SUBJECT TO A FULL EQUALITY IMPACT ASSESSMENT

Amendment Log

Version No	Type of Change	Date	Description of change
DRAFT		January 2014	
1		13 February 2014	*Approved by Governing Body*
2.0	Review	Jan 2016	*Personal email accounts removed from scope* *CSU references changed to commission support services / EMBED* *Section 7.1 requirement for specific email titles removed* *New NHSMail encrypted email service included* *Changes to improve clarity* *NHS Secure File Transfer service referenced*
3.0	Review	Mar 2018	*Updated References to DPA/GDPR* *Staff adherence to NHS Mail policies added.* *Removed claim to ownership of all information processed via email* *Removed approval required for ad-hoc transfers* *Removed requirement for delegate access to be read only* *Changes to sending confidential information and encryption.* *Restrictions on putting confidential information in calendar appointments* *Spam and Phishing Section added*

Contents

Section **Page**

Email Policy

1. Introduction

1.1 Email is an increasingly popular method of internal and external communication. It can be of great benefit to Barnsley NHS Clinical Commissioning Group (the CCG) when used appropriately. Its use, however, also exposes the CCG and individual users to new risks. These include legal action due to breaches of data protection and confidentiality requirements, threats to IT and information security, and ineffective communication. These risks and threats can compromise the CCG's ability to deliver effective care and services. Consideration should therefore be given to whether it is appropriate in any given situation to communicate by email.

1.2 Email is not always the best way to communicate information as email messages can often be misunderstood and the volume of email messages people receive can be prohibitive to receiving a meaningful reply as a result of email overload. Emails should be treated with the same level of attention that is given to drafting and managing formal letters and memos. As well as taking care over how email messages are written, emails should be managed appropriately after they have been sent or received.

1.3 This policy sets out the CCG's expectations of staff when using the email system, including accessing non-work email accounts on CCG systems. Procedural documents implementing this policy will be made available on the intranet. These documents and the policy itself should be cross-referenced with other information governance and procedural documents. An up to date list of documents will be made available on the information governance intranet page. Staff should ensure that they are familiar with the content of this policy and use it as a point of reference when dealing with email messages.

2. Objectives

2.1 The purpose of the policy is to aid staff in the effective and appropriate use of email on CCG systems and to reduce the risk of adverse events by:

- Setting out the rules governing the sending, receiving and storing of email.
- Establishing CCG and user rights and responsibilities for the use of its system.
- Promoting awareness of and adherence to current legal requirements and NHS information governance standards.

3. Scope

3.1 This policy applies to:

- NHS email accounts (*.nhs.uk and *.nhs.net) for business and personal use on CCG and non-CCG premises including from home, internet cafes and via portable media such as iPad and smart phones.
- All staff, in particular users of CCG systems and equipment including CCG employees and non-CCG employees who work within NHS

Barnsley Clinical Commissioning Group or under contract to it. This includes, but is not limited to, staff on secondment to the CCG, students on placement, commissioning support services staff working on behalf of Barnsley and people working in a voluntary capacity. (For convenience, the term 'staff' is used in this document to refer to all those to whom the policy applies.)

4. Compliance with this policy

- All staff are expected to comply with this policy as well as the NHS Mail policies and guidance published on the NHS Mail portal https://portal.nhs.net/Help/policyandguidance
- This policy is based on current law, NHS Information Governance standards and accepted standards of good practice; your **duty to handle CCG corporate and person confidential information appropriately** arises out of common law, legal obligations, staff employment contracts and professional obligations.[1]
- **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 also bring into question your professional registration and may result in disciplinary, civil or criminal proceedings**.
- If there is anything that isn't clear or which you do not understand in this policy you must contact your line manager, in the first instance, or the Information Governance Lead for further information.
- Please note that the procedures and policies outlined in this policy and any related policy may be changed at any time. You will be alerted to this via established CCG communication routes.

5. Generic Responsibilities of Staff and the CCG

- All managers are responsible for ensuring that the staff they manage are aware of the Email Policy and their individual responsibility for complying with it. They should ensure their staff are equipped to fulfil those responsibilities; this will include covering it at their local induction and by identifying and meeting specific and generic training needs through personal development plans.
- Managers should ensure ALL new staff have signed the Confidentiality and Information Security declaration. This should be done prior to giving them access to the CCG network. (The requirement to sign the declaration applies to ALL staff who work in the CCG and have access to CCG information and not only those with network access.) Managers are required to countersign this declaration to indicate that they have checked that the member of staff has read the relevant information governance policies and has had an opportunity to ask questions about anything they do not understand.

[1] For example, with the General Medical Council, Nursing and Midwifery Council or Health Professions Council

- Senior managers should ensure that managers within their Service are aware of their responsibilities in relation to informing staff about acceptable standards of information governance.
- The CCG allows short communications of a personal nature if it does not interfere with work. Although the personal use of email is discouraged due to the detrimental effect it may have on CCG business. (See section 7)
- All staff must ensure that they are aware of the requirements and standards of behaviour that apply, and adhere to this policy.
- All staff are responsible for reporting information incidents and near misses, including breaches of this policy, using the CCG's Incident Reporting procedures.
- The CCG's incident reporting process can be obtained from line managers in the first instance. Further information can be obtained from the CCG Quality Manager.
- The CCG's Information Governance Group is responsible for overseeing the implementation of this Email Policy including monitoring compliance. It is responsible for ensuring it is reviewed periodically.

6. CCG specific responsibilities and rights

6.1. Access to and use of email systems

- The CCG provides access to email systems to employees and authorised non-CCG employees only for use in their:
  - Work duties
  - Work related educational purposes
  - Work related research purposes
- No one has a right of access to an email account. The inappropriate use or abuse of email may result in access being withdrawn or amended.
- The CCG reserves the right to remove or amend access to the email system at any time in order to protect and preserve the integrity and confidentiality of the system.

The CCG will:

- Provide users with appropriate training in the use of email.
- Provide the appropriate and authorised software for email.

6.2. Monitoring

- All email used on local NHS systems is monitored for viruses, malware and spam
- All email (incoming and outgoing) on local NHS systems is logged automatically.
- Monitoring logs are audited periodically.
- The use of email is not private. The content of email is not routinely monitored but the CCG reserves the right to access, read, print or delete emails at any time.
- Any monitoring or interception of communications will be carried out in accordance with legislation such as the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice Practice) (Interception of Communications) Regulations 2000, the Data Protection Act, the General Data Protection Regulation, the Human Rights Act 1998 and specific procedures around monitoring and privacy.

6.3. Retention and destruction

- The CCG reserves the right to retain email as required to meet its legal obligations.

6.4. Investigating breaches of this policy

The CCG will:

- Investigate breaches of this policy, actual or suspected, in accordance with CCG procedures.
- Where appropriate, invoke the CCG's disciplinary procedure for breaches of this and the Fraud Bribery and Corruption Policy.
- Where appropriate, make a complaint to an individual's employing organisation and co-operate fully into any investigation of that complaint where breaches of this policy are committed by users who are not employees of the CCG (such as staff on secondment to the CCG, Honorary Contract holders and users given access to systems by agreement between the CCG and the user's employing organisation).
- Where appropriate take legal action (that is, criminal or civil proceedings) in respect of this policy.

6.5. Liability

- The CCG will not be liable for any financial or material loss to an individual when using email for personal use or when using personal equipment to access work email.

7. Staff specific responsibilities and rights

7.1. Access to and use of email systems

- Staff should use email only when it is appropriate to do so and not as a substitute for verbal communication.
- Emails should be worded with care because voice inflections cannot be picked up and it can be difficult to interpret tone.
- Email messages must not include anything that would offend or embarrass any reader or would embarrass the CCG if it found its way into the public domain.
- Write **ALL** emails on the assumption that they may be read by others, particularly people who do not normally work for the CCG such as temporary staff or staff in external organisations. Email is easily forwarded and may be read by unintended recipients.
- Staff must avoid putting confidential information in Calendar Appointments
- A concise meaningful title must be put in the subject heading of every email to indicate its content, whilst avoiding using over-dramatic ones.
- Users should not use email as the only method of communication if an urgent response is required.
- Where urgent information has been sent by email, confirmation of receipt should be obtained either by email or by a follow up telephone call.
- Users must access email regularly and respond to messages in a timely manner.
- Users should indicate when they are not able to read their email (for example, when on annual leave) using the tools within the email system.
- Users must only use disclaimers that have been authorised by the Communications Department.

Please note:

- Inappropriate use of email may result in poor communication, impede the function of the CCG's network system, impede the effective functioning of email, or compromise the security of the system.

7.2. Managing emails

- Email should be managed and stored in accordance with the CCG's Records Management Policy and other relevant policies.
- Email is a communication tool and not a records management system. Where the content of an email may be needed in the future it is the responsibility of the user to ensure it is stored appropriately (e.g. in network folders or printed out and added to manual records).
- Where the content of an email or attachments forms part of a record, it is the responsibility of the user to ensure the recorded is updated with the additional information, and that it becomes part of that record going forward.
- Emails and attachments that do not relate to work activities or do not need to be kept as part of a record must be deleted as soon as possible after receipt.

7.3. Legal requirements

- The use of email must comply with the law such as the Data Protection Act, the General Data Protection Regulation and adhere to CCG rules, codes of conduct, policies and procedures such as this policy and policies relating to equalities and anti-harassment.
- Users must comply with any licence conditions and copyright for any software they have access to.
- Users must not use email for any purpose that conflicts with their contract of employment.
- Users must not agree to terms or enter into contractual commitments or make representations by email without having obtained the proper authority. (A typed name at the end of an email is just as much a signature as if it had been signed personally.)
- Email messages have the same legal status as other written documents and must be disclosed in legal proceedings if relevant to the issues.
- The content of any emails may be disclosable under legislation such as the Data Protection Act, the Data Protection Regulation and the Freedom of Information Act 2000.
- Improper statements may result in the CCG and/ or user being liable under law.

7.4. Security

- All passwords and log in details for email systems must be kept confidential. Sharing passwords or log in details will be considered misconduct.
- Where necessary, users can give delegate access to their email account. Alternatively, a generic mailbox account can be set up with access via individual email accounts.)
- Users must lock their terminal when not at their computer (for example to make a cup of tea; to attend a meeting; or to go to lunch). To automatically lock the keyboard press the Windows key  and 'L' key at the same time or press Ctrl–Alt–Del, then choose 'lock computer').
- Any computer or portable device that is used for work purposes must be installed with up to date, approved anti-virus software. (Advice about anti-virus software can be obtained from the IT Service Desk.)
- Only portable devices, including tablet devices, mobile and smart phones, which are encrypted and are able to be remotely wiped should be used to access email.
- If email is downloaded onto portable devices, the device must not be synchronised with internet cloud storage services.

7.5. Sending, receiving and accessing confidential information by email

- Confidential or sensitive information, including information about patients/ service users and staff, must be encrypted if it is sent by email. To do so requires placing [secure] complete with square brackets, in the subject of the email to be protected. This applies to ALL emails, including those sent to email addresses outside of NHSMail.
  There are a number of other steps which must be followed to ensure confidentiality (such as test messages etc.). If you wish to use this facility you must follow the guidance which is available from NHSMail. *Sharing Sensitive Information:*
  https://portal.nhs.net/Help/policyandguidance
- Routine transfers of such information must be part of a work flow process and approved by the CCG's Information Governance (IG) Lead. Routine flows of personal information must be recorded in the dataflows register (see the IG Lead for information).
- There are several security issues associated with communicating with patients by email, it is difficult to authenticate the identity of patients; communication between the CCG and patients who are using a personal email account or an account from a non-secure domain will not, without additional steps, be secure.
  The CCG should only communicate with patients on matters of a confidential nature if they can verify the identity of the patient and the patient is made aware that email is not a secure method of communication and they consent and accept the risk. Services such as Complaints, who may have routine email contact with patients, should gain IG approval for the process as a whole but not individual communications.
- Personal confidential data such as names and addresses should not be included in the subject line of any emails.
- Safe haven procedures[2] must be considered when sending or receiving confidential or sensitive information by email.
- Confidential or sensitive CCG information must not be accessed from non-NHS equipment. (Arrangements for working outside of this policy require prior approval from the Senior Information Risk Owner, who should seek advice from the Information Governance Lead.)

[2] The sender should contact the intended recipient prior to sending the email to ensure it will be received in a timely manner (e.g. they are not ill or on annual leave); if it's a shared address that it's appropriate to send the information to it and to ask the recipient confirm its receipt.

7.6. Personal use

- The personal use of email is discouraged. If it is necessary to use NHS provided email systems for personal communications they must be brief, must not detract from the user's work duties and must not disrupt the work of others.
- Personal emails must adhere to the guidelines in this policy and must not breach any of the CCG's other policies or procedures
- Personal emails should be stored in a folder marked 'personal'.

7.7. Forwarding email

- Users must not automatically forward email from their CCG email account or send confidential or sensitive CCG information to non-NHS email accounts. Examples of non-NHS email accounts include Hotmail, Yahoo, Gmail, and email services provided by internet service providers.

7.8. Misuse of the system

Users must not:

- Use the CCG's email to conduct private or freelance work for the purpose of commercial gain.
- Create, hold, send or forward emails that have obscene, pornographic, sexually or racially offensive, defamatory, harassing or otherwise illegal content. (If you receive such a message you should report it to the IT Service Desk immediately.)
- Create, hold, send or forward emails that contain statements that are untrue, inaccurate, misleading or offensive about any person or CCG.
- Access and use another user's email account without permission. If it is necessary to access another user's account then contact the IT Service Desk for details of the necessary procedure. (Users should be aware that access to their email account by authorised individuals may be necessary in periods of absence for business continuity reasons.)
- Send email messages from another member of staff's email account (other than with delegated access) or under a name other than their own. Staff can give delegated access (proxy access) to their account and give permission for colleagues or administrative support to send emails on their behalf.
- Send global emails to ALL staff or to ALL GP practices. There are processes that must be followed for such communications. Contact the Communications Team for advice.
- Send unsolicited emails (spam) to large numbers of users unless it is directly relevant to the recipient's work. (Use staff bulletin/notice boards where appropriate.)
- Send emails to large numbers of users unless the recipients have been blind copied (bcc)[3]. (If the email is not blind copied, individual email addresses will be visible to everyone on the list which may compromise a recipient's confidentiality and take up a lot of space.)
- Send emails to a distribution list comprising members of the public unless the recipients have been blind copied (bcc)[3].

[3] To send a blind in Outlook In a message, click on the "Options" tab and in the "Show Fields" group, click Bcc. Place all recipients or the distribution list in the 'BCC:' field that will appear in the message window. The delivered email will suppress the list of other recipients.

- Use blind copying as a matter of course (except in the above circumstances) where its purpose is to withhold from the primary recipient the fact that an email has been copied to a third party. Communication should aim to be transparent and the use of blind copying in this manner an exception rather than the rule.
- Send or forward chain letters or other similar non-work related correspondence.
- Use email for political lobbying.
- Knowingly introduce to the system, or send an email or attachment, containing malicious software, e.g. viruses.
- Forge or attempt to forge email messages, for example, spoofing.
- Use instant messaging services, for example, Microsoft Messenger.

7.9. Sending attachments

- Users must not send or forward large messages or attachments. 10Mb is the absolute limit, but good practice is below 1-2Mb. The sending and storing of large attachments can adversely affect the CCG network (Examples of large attachments include photograph; office documents with other embedded files; electronic greetings and flyers.)
- Consider alternative ways of making large work documents available to colleagues such as placing documents on the intranet or a folder on the server and emailing a link. Alternatively, use other methods of file transfer, for example, the NHS Secure File Transfer[4] (Ask the IT Service Desk for advice.)

7.10. Reporting incidents

- Users must report serious incidents of unacceptable use, for example, obscene or racially offensive emails to their line manager or, where this is not possible, to the Head of Assurance directly. If in doubt, contact the EMBED IG Manager for advice.
- Any instances of suspected fraud should be referred to the Local Counter Fraud Specialist

8. Spam and Phishing Emails

- Staff must be aware of and avoid opening unwanted unsolicited emails known as Spam.
- Some unsolicited emails contain malicious web links which are intended to compromise network security and / or steal confidential information by masquerading as legitimate emails. These are known as Phishing emails.
- Where such emails have be opened inadvertently staff MUST NOT click on any links within the emails.
- Such emails can be forwarded **as an attachment only** to spamreports@nhs.net.
- Where a link in has been clicked in a suspected phishing or spam email, the IT Service Desk must be informed immediately.
- The *Cyber Security Guide* available on the NHSMail website https://portal.nhs.net/Help/policyandguidance contains further advice and guidance on dealing with threats via email.

[4] NHS Secure File Transfer https://nww.sft.nhs.uk/sft/upload1

9. Further information

- Further information about the policy can be obtained from the CCG's Information Governance Lead.
- Questions about the use of the system or any problems in accessing email should be directed to the IT Service Desk during opening hours. There is no out of hours or home support.

Equality Impact Assessment

Title of policy or service:	Email Policy	
Name and role of officer/s completing the assessment:	Gershon Nubour	
Date of assessment:	12 July 2018	
Type of EIA completed:	**Initial EIA 'Screening'** ☒ ***or*** **'Full' EIA process** ☐	*(select one option)*

1. Outline	
Give a brief summary of your policy or service • including partners, national or regional	Email Policy highlights expected standards when using CCG email systems including security and confidentiality and expected conduct
What Outcomes do you want to achieve	• Ensure information is handled appropriately and in a secure and confidential manner • Reduce the incidence and risk of adverse incidents and promote best practice • Compliance with expected standards when using email
Give details of evidence, data or research used to inform the analysis of impact	A draft of this policy has been circulated for review by the following:- • BCCGs Information Governance Group, • BCCGs Quality Patient Safety Committee, The final policy has been signed off by BCCGs Chief Nurse, the Head of Governance and Assurance and the Information Governance Manager (eMBED)
Give details of all consultation and engagement activities used to inform the analysis of impact	As above

Identifying impact:

- **Positive Impact:** will actively promote the standards and values of the CCG.
- **Neutral Impact:** where there are no notable consequences for any group;
- **Negative Impact:** negative or adverse impact: causes or fails to mitigate unacceptable behaviour. If such an impact is identified, the EIA should ensure, that as far as possible, it is eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information

This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.

(Please complete each area)	What key impact have you identified?			For impact identified (either positive or negative) give details below:	
	Positive Impact	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	☐	☒	☐		
Age	☐	☒	☐		
Carers	☐	☒	☐		
Disability	☐	☒	☐		
Sex	☐	☒	☐		
Race	☐	☒	☐		
Religion or Belief	☐	☒	☐		

Sexual Orientation	☐	☒	☐		
Gender Reassignment	☐	☒	☐		
Pregnancy and Maternity	☐	☒	☐		
Marriage and Civil Partnership (only eliminating discrimination)	☐	☒	☐		
Other Relevant Groups	☐	☒	☐		
HR Policies Only:	☐	☐	☐		

IMPORTANT NOTE: *If any of the above results in '**negative'** impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.*

Having detailed the actions you need to take, please transfer them to the action plan below.

3. Action plan				
Issues/impact identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication			
When will the proposal be reviewed and by whom?	The EIA will be reviewed when the policy is reviewed. The Head of Governance and Assurance is responsible for ensuring the review takes place.		
Lead / Reviewing Officer:	Richard Walker	**Date of next Review:**	March 2020

Once completed, this form **must** be emailed to the Equality Lead barnsleyccg.equality@nhs.net for sign off:

Equality Lead signature:
Date: