2019

Emailing Policy

DATA SECURITY AND PROTECTION TOOLKIT

Contents

1. Review

Version:	1.01
Approved By:	Mr Ahmad Syed
Date Approved:	
Review Date:	1 years from approval
Target Audience:	GP Practice

2. Introduction

2.1. Email is an increasingly popular method of internal and external communication. It can be of great benefit when used appropriately. Its use, however, also exposes GPs. practice staff and patient 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 practice's ability to deliver effective care and services. Consideration should therefore always be given to whether it is appropriate in any given situation to communicate by email.

2.2. 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.

2.3. This policy sets out the practice's expectations of staff when using the email system, including accessing non-work email accounts on CCG systems. This policy should be cross- referenced with other information governance and procedural documents. 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.

3. Objectives

3.1. The purpose of the policy is to aid staff in the effective and appropriate use of email and to reduce the risk of adverse events by:

3.1.1. Setting out the rules governing the sending, receiving and storing of email.

3.1.2. Establishing user rights and responsibilities for the use of its system.

3.1.3. Promoting awareness of and adherence to current legal requirements and NHS information governance standards.

4. Scope

4.1. This policy applies to:

4.1.1. NHS email accounts (*.nhs.uk and *.nhs.net) for business and personal use of these accounts in non-CCG premises including from home, internet cafes and via portable media such as ipads and smart phones.

4.1.2. It also applies to any NHS or other staff, who work in Pentelow Practice including staff on secondment or students on placement, commissioning support services staff working on behalf of the CCG, or those 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.)

5. Compliance with this policy

5.1. All staff are expected to comply with this policy.

5.2. This policy is based on current law, NHS Information Governance standards and accepted standards of good practice; your duty to handle practice administrative as well as person confidential information appropriately arises out of common law, legal obligations, staff employment contracts and professional obligations.[1]

5.3. Any breaches of this policy will be investigated in accordance employment processes and may result in disciplinary action, or referral to the Local Counter Fraud Specialist for further investigation and, if appropriate, your employment or association with the practice being terminated. It may also bring into question your professional registration[2] and may result in disciplinary, civil or criminal proceedings.

5.4. If there is anything that isn't clear or which you do not understand in this policy please contact the practice manager in the first instance, or the Information Governance Lead for further information.

5.5. Please note that the procedures and policies outlined in this policy and any related policy may be changed at any time, in which event you will be notified through the usual practice channels.

6. Generic Responsibilities of Staff and the practice

6.1. The partners and the practice manager 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.

6.2. Managers should ensure all new staff have signed the Confidentiality and Information Security clause in their contract. The practice manager will check 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.

6.3. The Caldicott Guardian should ensure that the practice manager is aware of their responsibilities in relation to informing staff about acceptable standards of information governance.

6.4. The practice allows short communications of a personal nature if it does not interfere with work. Although the personal use of email is discouraged in volume (See section 7)

6.5. All staff must ensure that they are aware of the requirements and standards of behaviour that apply, and adhere to this policy.

6.6. All staff are responsible for reporting information incidents and near misses, including breaches of this policy, to the Practice Manager who will document them via the practice Incident Reporting procedures.

6.7. The GP partners and practice manager are responsible for overseeing the implementation of this Email Policy including monitoring compliance. The practice manager is responsible for ensuring it is reviewed periodically.

7. Practice specific responsibilities and rights

7.1. Access to and use of email systems

7.1.1. The practice provides access to email systems to employees and authorised non practice employees only for use in their:

7.1.1.1. Work duties

7.1.1.2. Work related educational purposes

7.1.1.3. Work related research purposes

7.1.2. Although it will be our policy to issue email accounts to staff, this should not be considered a right. The inappropriate use or abuse of email may result in access being withdrawn or amended.

7.1.3. The practice 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.

7.2. The practice and the CCG IT team will:

7.2.1. Provide users with appropriate training in the use of email.

7.2.2. Provide the appropriate and authorised software for email.

7.3. Monitoring

7.3.1. Any information held or passing through the practice’s email system is the property of the practice.

7.3.2. All email used on local NHS systems is monitored for viruses and malware.

7.3.3. All email (incoming and outgoing) on NHS systems is logged automatically via NHS email.

7.3.4. Monitoring of logs may be audited periodically.

7.3.5. The use of email is not private. The content of email is not routinely monitored but the practice reserves the right to access, read, print or delete emails at any time.

7.3.6. 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 2018, the Human Rights Act 1998 and specific procedures around monitoring and privacy under GDPR.

7.4. Retention and destruction

7.4.1. The practice reserves the right to retain email as required to meet its legal obligations.

7.5. Investigating breaches of this policy the practice will:

7.5.1.Investigate breaches of this policy, actual or suspected, in accordance with practice procedures.

7.5.2.Where appropriate, invoke the practice’s disciplinary procedure for breaches of this and the Fraud Bribery and Corruption Policy.

7.5.3.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 practice (such as staff on secondment to the practice, Honorary Contract holders and users given access to systems by agreement between the practice and the user’s employing organisation).

7.5.4.Where appropriate take legal action (that is, criminal or civil proceedings) in respect of this policy.

7.6. Liability

7.6.1.The Practice 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.

8. Staff specific responsibilities and rights

8.1. Access to and use of email systems

8.1.1. Users should use email only when it is appropriate to do so and not as a substitute for verbal communication.

8.1.2. Emails should be worded with care because voice inflections cannot be picked up and it can be difficult to interpret tone.

8.1.3.Email messages must not include anything that would offend or embarrass any reader or would embarrass the Practice if it found its way into the public domain.

8.1.4. All emails should be written on the assumption that they may be read by others, particularly people who do not normally work for the practice, such as temporary staff or staff in external organisations. Email is easily forwarded and may be read by unintended recipients.

8.1.5. A concise meaningful title must be put in the subject heading of every email to indicate its content, whilst avoiding using over-dramatic ones.

8.1.6. Users should not use email as the only method of communication if an urgent response is required.

8.1.7. Where urgent information has been sent by email, confirmation of receipt should be obtained either by email or by a follow up telephone call.

8.1.8. Users must access email regularly and respond to messages in a timely manner.

8.1.9. 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.

Please note: Inappropriate use of email may result in poor communication, impede the function of the practices communication systems, impede the effective functioning of email, or compromise the security of the system.

8.2. Managing emails including those with clinical content

8.2.1. Email should be managed and stored in accordance with the Practice's Records Management Policy and other relevant policies.

8.2.2. Email is intended as communication tool rather than 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 or electronic records).

8.2.3. Where the content of an email or attachments forms part of a clinical patient record, it is the responsibility of the recipient to ensure the recorded is updated with the additional information, and that it becomes part of that record going forward. In respect of this requirement the sender, the recipient, the time of sending the title and content of the email should be recorded by cutting and pasting (or by attachments where appropriate) into a clinical entry, which under consultation type within the clinical system should be documented as being an email communication

8.2.4. Wherever possible, third party data should not be attached to a clinical record and if the user is in doubt about this, they should seek advice from the senior receptionist, practice manager, clinician or Caldicot guardian. In the event that it is necessary to record third party information, the type of consultation within the clinical system should be documented as being a third party consultation (so as to make this easily identifiable when needed) and a read code for email consultation should be added.

8.2.5. When an email which contains relevant clinical information needs to be recorded in the patient record, all the required information should be transferred and at the conclusion of that process, the original email should be deleted. The deleted items box should also be deleted daily.

8.2.6. In the event of an email containing clinical information which requires a delegated action, the user should transfer the contents to the patient record, delete the email and message the action to the required member(s) of staff using their preferred management system (for example a task within SystmOne).

8.2.7. Forwarding emails which contain clinical data should be avoided. But where it is considered necessary the forwarder should indicate to the recipient that either:

8.2.7.1. They have updated the clinical record and deleted the original email, and that the recipient can and should delete their copy of the email when actioned.

Or

8.2.7.2. That that have not updated the clinical record and that it is the responsibility of the recipient to do so and to subsequently delete their copy of the email.

8.2.7.3. In the event of either a) or b) the person forwarding the email should always delete the email from their own email account.

8.2.8. Where shared email accounts are used (such as a practice email which may be available to more than one person), there should be a clear line of accountability and ownership so that a single named member of staff is held responsible for managing the account over any given time period or rota. Staff who may have access to shared emails and who read them should either action, transfer, delegate and delete (as above), or having viewed the email they should subsequently mark it as unread, so that the owner of the account is aware of which emails need processing

8.2.9. Emails and attachments that do not relate to work activities or do not need to be kept as part of a record must also be deleted as soon as possible after receipt.

8.3. Legal requirements

8.3.1. The use of email must comply with the law such as the Data Protection Act 2018 and adhere to practice rules, codes of conduct, policies and procedures such as this policy and policies relating to equalities and anti-harassment.

8.3.2. Users must comply with any licence conditions and copyright for any software they have access to.

8.3.3. Users must not use email for any purpose that conflicts with their contract of employment.

8.3.4. 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.)

8.3.5. Email messages have the same legal status as other written documents and must be disclosed in legal proceedings if relevant to the issues.

8.3.6. The content of any emails may be disclosable under legislation such as the Data Protection Act 2018 and Freedom of Information Act 2000.

8.3.7. Improper statements may result in the practice and/or user being liable under law.

8.4. Security

8.4.1. 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 proxy access to their email account. This should be read access only. Alternatively, a generic mailbox account can be set up with access via individual email accounts.)

8.4.2. Users must lock their terminal when briefly not at their computer (for example to make a cup of tea; or a toilet break). The system should be set to have an automatic screen lock where there is no use for a given period of time. To manually lock the keyboard press the Windows key ⊞ and 'L' key at the same time or press Ctrl–Alt–Del, then choose 'lock computer'). For longer breaks such as attending a meeting; or going to lunch the user should always log out of the system and remove their smartcard.

8.4.3. In setting at reception where there are more than two receptionists and only two screens it is acceptable to share reception log in only if the user informs the smart card user (who is always ultimately responsible) of actions taken and also when entering clinical data in a patient record that they document their use and identity manually.

8.4.4. Any computer or portable device that is used for work purposes must be installed with up to date, approved anti-virus software. (This will usually be managed by the IT team and supported through the IT Service Desk.)

8.4.5. 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.

8.4.6. If email is downloaded onto portable devices, the device must not be synchronised with internet cloud storage services.

8.4.7. USB devices (including iphones) which have not been approved by the IT team should never be attached to the clinical system or work PCs.

8.5. Sending, receiving and accessing confidential information by email

8.5.1. Confidential or sensitive information, including information about patients/service users and staff, must be encrypted if it is sent by email[3]. Routine transfers of such information must be part of a work flow process and approved by the Information Governance (IG) Lead. Routine flows of personal information must be recorded in an information map (see the IG Lead for information). Approval for ad hoc transfers of confidential information should be obtained from the IG Lead.

8.5.2. It is now possible to send secure encrypted messages to email addresses outside of the secure government ones listed in the footnotes. To do so requires placing [secure] complete with square brackets, in the subject of the email to be protected. There are a number of other steps which must be followed to ensure security (such as test messages etc.). If you wish to use this facility you must follow the guidance which is available on the NHSMail website[4].

8.5.3. There are several security issues associated with communicating with patients by email, it is important to authenticate the identity of patients; communication between the practice 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 practice 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 the email is not secure and they consent.

8.5.4. Personal confidential data such as names and addresses, should not be included in the subject line of any emails.

8.5.5. Safe haven procedures[5] must be used when sending or receiving confidential or sensitive information by email.

8.5.6. Confidential or sensitive practice information must not be accessed from non-NHS equipment. (Arrangements for working outside of this policy require prior approval from the practice manager or Caldicott guardian/ Information Governance Lead.)

[3] Emails sent between *.nhs.net accounts and the accounts listed below are encrypted in transmission (but not at the end point so care must be taken to send emails to the correct address):

# NHS (*.nhs.net) # GCSX (*.gcsx.gov.uk)

# GSI (*.gsi.gov.uk) # SCN (*scn.gov.uk

# CJX (*.police.uk or .pnn.police.uk) # CJSM (*cjsm.net)

# GSE (*.gse.gov.uk) # MoD (*.mod.uk) #

GSX (*.gsx.gov.uk)

Local Authority staff can register for GCSX email.

[4] Encryption guidance for NHSmail users: https://web.nhs.net/public/InformationGuidanceServices/DefaultPage.aspx

[5] 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

8.6. Personal use

8.6.1. 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.

8.6.2. Personal emails must adhere to the guidelines in this policy and must not breach any practice policies or procedures

8.6.3. Personal emails should be stored in a folder marked 'personal'.

8.7. Forwarding email

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

8.8. Misuse of the system Users must not:

8.8.1. Use practice email to conduct private or freelance work for the purpose of commercial gain.

8.8.2. 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 Practice manager immediately.)

8.8.3. Create, hold, send or forward emails that contain statements that are untrue, inaccurate, misleading or offensive about any person or organisation.

8.8.4. 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.)

8.8.5. 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.

8.8.6. Send global emails to ALL staff or to ALL GP practices. There are processes that must be followed for such communications. Contact the Practice Manager for advice.

8.8.7. 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.)

8.8.8. Send emails to large numbers of users unless the recipients have been blind copied (bcc)[6]. (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.)

8.8.9. Send emails to a distribution list comprising members of the public unless the recipients have been blind copied (bcc)[6].

8.8.10. 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.

8.8.11. Send or forward chain letters or other similar non-work related correspondence.

8.8.12. Use email for political lobbying.

8.8.13. Knowingly introduce to the system, or send an email or attachment, containing malicious software, e.g. viruses.

8.8.14. Forge or attempt to forge email messages, for example, spoofing.

8.8.15. Use instant messaging services, for example, Microsoft Messenger.

8.9. Sending attachments

8.9.1. Users must not send or forward large messages or attachments. 10Mb is a practical limit and whilst it may be possible to send larger emails this is not good practice unless absolutely required. In general staff should aim to send emails no larger than 1-2 2Mb. The sending and storing of large attachments can adversely affect the practice and the NHS network. 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[7] (Ask the IT Service Desk for advice.)

8.10. Reporting incidents

8.10.1. Users must report serious incidents of unacceptable use, for example, obscene or racially offensive emails to their practice manager.

8.10.2. Any instances of suspected fraud should be referred to the practice manager who will contact the Local Counter Fraud Specialist

[6] 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.

9. Further information

9.1. Further information about the policy can be obtained from the practice’s Information Governance Lead.

9.2. 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.

[7] NHS Secure File Transfer https://digital.nhs.uk/services/transfer-data-securely