NHS
Stockport
Clinical Commissioning Group

# Email Policy

Version 1.1

***NHS Stockport Clinical Commissioning Group*** will allow people to access health services that empower them to live healthier, longer and more independent lives.

**NHS Stockport Clinical Commissioning Group**
7th Floor
Regent House
Heaton Lane
Stockport
SK4 1BS

**Tel:** 0161 426 9900 **Fax:** 0161 426 5999
**Text Relay:** 18001 + 0161 426 9900

**Website:** www.stockportccg.org

<table>
<tr><td colspan="3">**Document title :**</td><td>**Policy No:**</td><td>**Version No.**</td></tr>
<tr><td colspan="3">Email Policy</td><td>IG09</td><td>1.0</td></tr>
<tr><td colspan="5">**Staff Group covered by this document:**</td></tr>
<tr><td colspan="5">All NHS Stockport CCG employees and contracted staff, any staff on placement (including students, trainees, seconded staff), Governing Body members.</td></tr>
<tr><td colspan="5">**Key Objectives of the document:**</td></tr>
<tr><td colspan="5">To ensure safe and secure use of email.<br>To help users unlock the benefits of the new email system.<br>To reduce the risk of data loss.</td></tr>
<tr><td colspan="5">**Ratification:**</td></tr>
<tr><td colspan="5">NHS Stockport CCG Information Governance Group</td></tr>
<tr><td colspan="5">**References / Bibliography and Associated Documents:**</td></tr>
<tr><td colspan="5">NHS Stockport CCG – Acceptable Use of IT Policy<br>NHS Stockport CCG - Information Security Policy<br>NHS Stockport CCG - Information Governance Assurance Framework<br>NHS Stockport CCG - Procedure for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents (SUIs)<br>NHS Stockport CCG - Safe Haven Guidance<br>GMCSU – Corporate Information Security Policy<br>NHS Mail Acceptable use policy</td></tr>
<tr><td>**Signed off by:**</td><td colspan="4">Gaynor Mullins</td></tr>
<tr><td>**Position:**</td><td colspan="4">Chief Operating Office</td></tr>
<tr><td>**Date:**</td><td colspan="4">10 March 2014<br>***A hard copy of this cover page containing a wet signature is held on file by the Head of Compliance.***</td></tr>
<tr><td colspan="2">**Date of issue:**</td><td colspan="3">**Accountable Director:**</td></tr>
<tr><td colspan="2">10 March 2014</td><td colspan="3">Gary Jones, Chief Finance Officer</td></tr>
<tr><td colspan="2">**Date of Next Review:**</td><td colspan="3">**Responsible Committee or Officer:**</td></tr>
<tr><td colspan="2">March 2015</td><td colspan="3">IG Group (write)<br>Directors meeting (sign-off)</td></tr>
<tr><td colspan="5">**Distribution:**</td></tr>
<tr><td colspan="5">NHS Stockport SharePoint intranet site.<br>*Please note that the SharePoint version of this document is the only version that is maintained. Any printed copies should therefore be viewed as “uncontrolled” and as such, may not necessarily contain the latest updates and amendments.*</td></tr>
</table>

## Contents

## 1. Introduction

NHS Stockport CCG uses the centrally hosted NHS Mail system. NHS Mail offers many benefits to users including;

- Endorsement from the BMA and RCN for the exchange of clinical data (see section 9)
- Free SMS and Fax facility. Ability to link to systems for automated SMS texting of patient appointment reminders and other messages.
- Ability to access your email from home and on compliant mobile devices (eg iPhones, smartphones) with a remote wipe facility if the device is lost.
- Replaces many paper based, phone and manual processes to streamline workflow and improve patient care.
- Stockport Community staff, GPs, CCG staff and participating pharmacists, optometrists and dentists all on one secure email system.
- Secure, resilient and robust centralised system.
- Removes the need for a locally hosted and costly system.

## 2. Purpose

2.1. This document outlines the email policy for NHS Stockport CCG users. The document is intended to be read and understood easily by users of email within NHS Stockport CCG and to outline acceptable and unacceptable use of the email system.

2.2. The document will also give guidance to users on best practice use of email but is not intended to be a training guide. Training and guidance is available online or through the IT Service Desk

## 3. Scope

3.1. This policy applies to;

- All NHS Stockport CCG employees and contract staff.
- Any staff on placement (including students, trainees, secondees)
- Non-executive directors
- Hosted services staff

- Partners accessing NHS Mail through the NHS Stockport CCG network.

3.2. For GP surgeries, this policy should work in conjunction with local policies. Elements of this policy will apply to GP surgeries by default through the technical configuration of the email system.

## 4. Legal Risks

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

- If you send emails with any libellous, defamatory, offensive, racist or obscene remarks, you and the CCG can be held liable.
- If you forward emails with any libellous, defamatory, offensive, racist or obscene remarks, you and the CCG can be held liable.
- If you send or forward emails that may constitute sexual harassment, you and the CCG can be held liable.
- If you unlawfully forward confidential information, you and the CCG can be held liable.
- If you unlawfully forward or copy messages without permission, you and the CCG can be held liable for copyright infringement.
- If you send an attachment that contains a virus, you and the CCG can be held liable.

## 5. Responsibilities

5.1. The CCG is responsible for making users aware of the training available for NHS Mail. The CCG will take all reasonable steps to ensure that users are aware of the relevant policies, protocols, procedures and legal obligations relating to the use of email.

5.2. Managers are responsible for ensuring that their staff are aware of the policy and that the policy is enforced.

5.3. Managers are responsible for ensuring that the IT Service Desk are made aware of starters and leavers for the set up and closure of NHS Mail accounts. Timely notification of leavers is more important than ever, as an NHS Mail account can be accessed on any PC or device with an internet connection.

5.4. Employees and those in scope are responsible for following this email policy in accordance with the CCG's code of conduct.

5.5. Employees are responsible for keeping their password secure and ensuring it is only known to them.

## 6. Accessing your email

6.1. Each member of staff should be set up with an NHS Mail email account. NHS Mail can be accessed either through Outlook or through a web page (www.nhs.net). Web access to NHS Mail is available from any internet connected computer, although functionality is restricted when you are not on an NHS network, for example, locked accounts cannot be unlocked outside of the NHS network (N3).

6.2. When logging on to NHS Mail outside of CCG buildings,  the following precautions must be taken:

- Do not access your mailbox on a public use computer eg in a coffee shop, library or internet cafe.
- Do not access your mailbox through a public wi fi or public internet connection unless you are using a secure VPN token (available through IT procurement).
- If you are connecting using a home wireless connection make sure your home network is password protected with a WiFi Protected Access (WPA) or Wireless Encryption Protocol (WEP) security key. For more information contact your internet provider.
- When accessing your mailbox outside of the NHS network, always select the public default option before logging in.
- Make sure that no one watches you type your username and password when you log in and that no one can see your screen whilst working.
- Do not select an option that allows you to save your password for later use.
- Only provide your username and password to the NHSmail website, do not respond to any emails asking you to provide your password.

- Do not save, copy, cache or screenshot any sensitive or identifiable data onto a non-Trust computer or non-Trust network share.
- Do not integrate your NHS Mail account with an email program (such as Microsoft Outlook or Apple Mail) on a non-Trust computer.

6.3. When using NHS Mail through the web browser window, always make sure you **log out** before closing the window.

## 7. Password management

7.1. Your password is a key component in the security of the NHSmail service. You are responsible for keeping it safe and secure. Do not write it down or record it anywhere where someone could access it.

7.2. Do not divulge to anyone else, your password or security questions.

7.3. If you think your password is known to others you should change it immediately, either through the web access to NHS net for self service, or through the service desk if you are not on an NHS network connected computer.

TIP

If you use a mobile device, make sure you change the saved NHS Mail password on the device if you change your email password, otherwise it will stop receiving and sending emails.

## 8. Use of email

8.1. Email should be used for clinical and business use only. The following commercial uses are expressly prohibited;

- Advertising for or promotion of personal business(es).
- Solicitation to buy or sell goods or services for personal profit.

8.2. Users should not register their NHS email address with websites or other bodies that are not related to NHS business. Users should not publish their email address online, for example on social networking websites, unless it is directly linked to CCG business. In this situation prior management approval is required.

8.3. Chain letters and jokes are classed as junk mail and should not be forwarded. This can drain network resources, cause offence/distress and affect user quota limits.

8.4. Large attachments can affect the CCG network and reduce a user’s mailbox quota. A large attachment is classed as anything over 500kb. Users should embed links to files wherever possible instead of attaching files.

## 9. Sending patient or personal identifiable data

9.1. No patient identifiable information should be sent via NHS Mail to addresses not ending in:

@nhs.net;.x.gsi.gov.uk; .gsi.gov.uk; .gse.gov.uk; .gsx.gov.uk; .police.uk; .pnn.police.uk; .cjsm.net; .scn.gov.uk; .gcsx.gov.uk, .mod.uk

9.2. You should ensure that relevant patient data contained in emails is immediately attached to the patient record in the relevant clinical system. Failure to do so could have implications for patient safety. Once stored in the patient record, patient identifiable data should be deleted from NHS Mail.

9.3. When sending patient or personal identifiable data via email, ideally, the patient's NHS number should be used as the identifier. If the NHS Number cannot be used, as a last resort, only 2 key identifiers must be used. Key identifiers are Name, DOB or Address. [Appendix 1].

9.4. When sending patient/ personal identifiable or sensitive data via email always double check that the address you are sending to is correct and request a delivery and read receipt. Many NHS staff will have the same name and their email address will be in a different format, for example john.smith@nhs.net, johnsmith@nhs.net, john.smith1@nhs.net etc.

## 10. Emails to patients

10.1. If patients email the CCG or practices they must be made aware that any email content between the Trust and themselves will not be encrypted or secure and that they should not send content they consider as private and confidential.

If it is critical to patient care or if the patient is willing to accept the security risks and gives express consent to communicate sensitive data over email then it is acceptable to send sensitive data over email to patients.

## 11. SMS texts to patients

11.1. NHS Mail offers the ability to send email to SMS text. The service is free of charge. Users should not use this facility to send personal texts as it is a business system and should be used only for organisational or clinical purposes.

11.2. No personal or patient identifiable information should be sent via text.

11.3. Patients can be contacted by text by practices or services. This could be through automated reminders or targeted group messaging, for flu priority patients for example. The patient must give consent when they share their mobile number with the practice or service and be made aware that they may be contacted by text with appointment reminders or general health related messages.

**T I P**

To send a text through NHS mail type the number followed by @sms.nhs.net in the 'to' field. Eg; **0798989112@SMS.nhs.net**

To send a fax, do the same but use **@Fax.nhs.net** after the number

## 12. Generic team/service/practice mailboxes

12.1. Generic mailboxes can be set up for teams, services, practices or functions. They are designed to be accessible by a number of delegated staff. Staff can access the shared mailbox via their own personal account and there is an audit trail for security purposes.

12.2. The generic mailbox address has a stockport (sto-ccg) prefix, eg;

**sto-ccg.*Yourservicename*@nhs.net**

12.3. In some circumstances teams/services/practices may require a named account such as *yourservicename@nhs.net* as it is easier to remember. Such accounts can be set up, but there must be a named owner of the account who is responsible and accountable for the use of the mailbox.

In the case of these generically named accounts, delegated mailbox access should be given to relevant staff, rather than simply giving multiple staff the username and password, which contravenes the NHS Mail acceptable use policy.

## 13. Email to fax facility

13.1. NHS Mail offers a free email to fax facility. Staff should utilise this functionality where appropriate to streamline processes and reduce the use of fax machines along with the costs associated with them.

13.2. Users should follow IG guidelines and approach fax sending in the same way as they would when sending a fax by conventional methods. (see appendix 3)

## 14. Audit and monitoring

14.1. Email accounts are scanned for viruses and offensive content. At the request of the line manager a mailbox can be suspended and audited as part of a disciplinary investigation. Managers must contact the IT Service Desk to initiate the disciplinary process before a mailbox can be audited.

14.2. A Mailbox can be suspended immediately if the line manager suspects one of their staff is involved in a major security/confidentiality breach or gross misconduct. The line manager must inform the IT Service Desk via email, including the name of the staff member.

## 15. Attachments

15.1. Only open attachments from people you know and trust.

15.2. Only save attachments containing personal or patient identifiable and organisationally sensitive information to secure network storage drives. Be aware that any data saved elsewhere is unsecured and isn't backed up.

15.3. Attachments can be up to 20MB in size.

15.4. A number of file types such as MP3s and MPEG movies are blocked for sending and receiving. See appendix 2 for a full list of blocked file types.

## 16. Personal Folders

16.1. Personal folders can be set up to file and store messages.

16.2. Personal folders should be stored in a secure and backed up area on the network. If in doubt, contact the IT Service Desk. If you store them elsewhere, the emails are prone to loss and/or data security breaches.

16.3. Personal folders should be reasonable in size and never exceed 20GB. If a folder does exceed 20GB it is prone to corruption and you could lose the emails contained within it.

16.4. Users should be aware that personal folders take up network storage at a cost to the CCG and should only keep and store what is necessary, both for legal reasons and for effective clinical and business performance.

## 17. Email quotas

17.1. Email quotas are in place because network storage is not unlimited and has costs associated to it.

17.2. Each user is given a Silver quota mail box by default (see below 17.4). Each directorate or service is granted an allocation of each mailbox size. It is up to the service leads to decide how their allocations are set, as they will know their key users. Users who require an upgrade to a larger mailbox must request this via their director or associate director.

17.3. Users must perform regular housekeeping on their mailbox to keep it at a manageable level.

17.4. The quota sizes are as follows;

| | |
|---|---|
| Bronze | 100 MB |
| Silver | 400 MB |
| Gold | 1 GB |
| Platinum | 2 GB |

## 18. Secure transfer of files

18.1. Secure File Transfer (SFT) offers the ability to send files and data, up to 1GB in size, securely, by password protecting them. This facility can replace the sending of CDs and other transferable media.

Both the sender and receiver must have an NHS.Net account. The password can be sent automatically to the receiver's mobile phone or manually by email or text, after which they will be able to open the file on their computer.

For more information and to register, go to https://nww.sft.nhs.uk

## 19. Internet Email

19.1. Internet email websites such as Google mail (Gmail), Hotmail and Yahoo Mail should not be accessed on Trust connected computers. Use of such accounts increases the threat of viruses to the Trust and practices. There are also Information Governance risks associated with the use of internet email accounts.

This does not impact on emails received from and sent to internet email addresses.

## 20. Non Compliance

Failure to observe this policy and associated protocols and procedures may be regarded by the CCG as gross misconduct. Disciplinary procedures, civil action or criminal proceedings may be instigated as a consequence of damage caused to an individual, the CCG or its partner organization by non-compliance with this policy. Please see the HR Disciplinary Policy and Code of Conduct located on SharePoint for further details.

## 21. Training and dissemination

Promotion, awareness and training will be achieved using the following methods:

- Distribution of the policy via SharePoint.
- Distribution of the policy to practices and 3rd party contractors via CCG business managers.
- News item on team brief.
- Drop in sessions will be held, where possible, to increase awareness of the policy.
- The policy will be incorporated into formal IM&T induction and training.

## 22. More information

Up to date information, FAQs, NHS wide policy and guidance can be found on the NHS.net website using the link below (requires you to login to NHS.net with your email account credentials);

https://web.nhs.net/Portal/InformationGuidanceServices/DefaultPage.aspx

## Appendices

### Appendix 1

**NHS Number - Key Identifier**

The NHS has been charged with achieving complete adoption of the new NHS Number as defined and monitored in the priorities of the NHS Operating Framework to meet the requirements of the NHS  Number Operational Information Standards for the NHS in England published by the Information Standards Board (ISB) in December 2008 together with associated Data Set Change Notices.

The four major principles in the complete adoption and use of the NHS Number as the only national unique patient identifier in operation in the NHS at this time are:

- The NHS Number will be included as a key patient identifier on all systems and documents which include Patient Identifiable Data.
- The NHS Number will be the “first choice” for searching electronic patient records.
- All practical attempts should be made to determine the NHS Number before or at the start of an episode of care, but if this is not possible then tracing should be performed as early as possible in the episode.
- The NHS Number will be supplied as a key patient identifier for any Patient Identifiable Data that passes across system or organisational boundaries.

If the NHS Number can not be used as a last resort only 2 key identifiers must be used.  Key identifiers are Name, DOB or Address.

For further details please read the NHS Number Strategy and the Safe Haven Guidance which are both on SharePoint.

## Appendix 2 – Blocked File attachment types

| File type | Description |
|---|---|
| 7zip | File archiver with high compression ratio |
| Avi | Audio Video Interleaved animation file |
| Bas | BASIC programming files |
| Bat | DOS batch file |
| Chm | MS compiled HTML help file |
| Cmd | OS/2 or Windows NT batch file |
| Cnt | Helpfile contents |
| Com | 16-bit DOS executable |
| Cpl | Windows Control Panel extension |
| Crt | Security Certificate |
| Eml | Outlook Express mail message |
| Exe | DOS or Windows 16/32 bit executable |
| Hlp | Windows help files: 16-bit executable |
| Hta | HTML file |
| Inf | Windows installer setup file - 16-bit executable |
| Ins | Internet naming service |
| Isp | Internet communication settings |
| Js | JavaScript file. |
| Jse | JavaScript encoded script |
| Lnk | Windows shortcut file |
| Mpe | MPEG Movie Clip |
| Mpeg | MPEG Movie Clip |
| Mpg | MPEG animation |
| mp2 | MPEG audio file |
| mp3 | mp3PRO Audio file |
| Msc | MS common console doc |
| Msi | Windows installer file |
| Msp | Windows installer patch |
| Mst | Visual test source file |
| Pcd | Photo CD image` |
| Pif | Program Information File |

## Appendix 3 – Safe Haven fax guidance

### Transmission of Personal Information via Fax

- Fax machines must only be used to transfer personal information where it is absolutely necessary to do so.
- Safe Haven fax machines must be placed in a secure location and are lockable when unattended. Ideally they should require a code password or pin for operation. Numbers for these dedicated fax machines must be made known.
- The following rules apply:
- You have clarified with the intended recipient that they operate safe haven procedures in a location where only staff that have a legitimate right to view the information can access it.
- The sender is certain that the correct person will receive it and that the fax number is correct (confirm with the individual if you are unsure).
- You notify the recipient when you are sending the fax and ask them to acknowledge receipt of the information and number of indicated pages.
- Care is taken in dialling the correct number. Frequently used numbers should be pre-programmed to reduce misdialling. Pre-programmed numbers should be routinely checked for accuracy.
- Confidential faxes are not left lying around for unauthorised staff / members of the public to see.
- Only the minimum amount of personal information should be sent. Where possible, the data should be anonymised or NHS Number unique identifier used. Where both clinical and personal data is essential to be sent, you should consider sending them separately, ensuring the first fax has been received prior to sending the remainder.
- Faxes sent should include a CCG front sheet which states ‘Private and Confidential’ and which contains the CCG confidentiality and disclaimer clause. The intended recipient’s name and job title should be clearly included. Do not include any sensitive information on the front sheet.
- A ‘sent report’ should be obtained which is evidence that your fax was sent to the correct fax number and received by the fax at the other end. This report should be kept secure as part of an audit trail.
- Never leave the information unattended whilst it is being transmitted.
- Do not send a fax to a destination where you know it is not going to be seen for some time or outside office opening times (whenever possible).
- NHS Mail offers a free email to fax facility. Staff should utilize this functionality where appropriate to reduce the use of fax machines and the costs associated with them.
- Users should follow IG Guidelines and approach fax sending in the same way as they would when sending a fax by the conventional methods.

## Equality Impact Assessment – Relevance Screening

| | | | | | |
|---|---|---|---|---|---|
| 1. | **Name of the Policy*:** | Email Policy | | | |
| 2. | **Person Responsible:** | Paul Fleming | | | |
| 3. | **What are the main aims of the Policy*?** | To ensure safe and secure use of email.<br>To help users unlock the benefits of the new email system.<br>To reduce the risk of data loss. | | | |
| 4. | **Is this a strategic document or a major project?** | **YES** | | **NO** | |
| | | | | ✓ | |
| 5.a | **What type of impact is this Policy* likely to have on staff or service users from the following equality groups?** | **HIGH** | **MEDIUM** | **LOW** | **DON'T KNOW** |
| | **Age** | | | ✓ | |
| | **Carers** | | | ✓ | |
| | **Disability** | | | ✓ | |
| | **Ethnicity** | | | ✓ | |
| | **Gender** | | | ✓ | |
| | **Gender Reassignment** | | | ✓ | |
| | **Pregnancy & Maternity** | | | ✓ | |
| | **Religion & Belief** | | | ✓ | |
| | **Sexual Orientation** | | | ✓ | |
| 5.b | **Please explain your answer:** | The changes in system and policy have little impact on different equality groups. | | | |

If you have answered YES to question 4, and:

- HIGH impact in 5a - you should move on to a FULL Equality Impact Assessment.
- MEDIUM / LOW / DON'T KNOW in 5a - you should move on to an INITIAL Equality Impact Assessment.

If you have answered NO to question 4, and:

- HIGH / MEDIUM / DON'T KNOW in 5a, you should move on to an INITIAL Equality Impact Assessment.
- LOW impact in 5a, you do not need to complete an Equality Impact Assessment.

| | | | | |
|---|---|---|---|---|
| 6. | **Based on this screening, please indicate if this should proceed to an Initial or Full EIA?** | **INITIAL** | **FULL** | **NONE** |
| | | | | ✓ |
| 7. | **Date of EIA Approval:** | | | |

* The term 'Policy' in this context is used to cover any of the following:

Policy / Procedure / Guidelines / Protocol / Service / Practice / Project / or Strategy