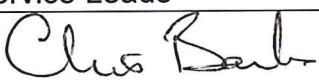


Tower Hamlets GP Care Group Email Usage Policy

Date Issued	
Date to be reviewed	Periodically or if statutory changes are required
Title	Email Usage Policy
Supersedes	All previous Policies
This policy will impact on	All staff
Financial Implications	No change
Policy Area	Information Governance
Version No	1.1
Issued By	Quality, Safety & Governance Team
Author	Ruth Walters
Document Reference	
Effective Date	
Review Date	

Approval Record

	Committees / Groups / Individual	Date
Consultation	Quality, Safety & Governance Committee, Service Leads	February/March 2018
Approved by		5/4/2018



Scope

This policy applies to all employees at the Care Group (including contractors and Board members) and anyone who has been granted access to a THGPCG NHS net account as part of an honorary contract.

Introduction

The Care Group uses NHSmail and this policy sets out the conditions of use for employees.

The NHSmail service has been provided to aid the provision of health and social care and this should be employees main use of the service.

It can be acceptable for a designated and authorised individual to view the contents of another's files and folders within NHSmail, for example a secretary or PA.

Clinical staff are permitted to use the NHSmail service in relation to the treatment of private patients in accordance with the relevant professional codes of conduct.

NHS staff contact details are provided in the NHS Directory to support the delivery of healthcare and these details will be shared across the NHS.

NHSmail accounts are owned by NHS Digital on behalf of the Secretary of State for Health and provided to employees for their use.

The NHSmail programme reserves the right to withdraw an email account from use should operational requirements dictate.

Employee responsibilities when using the service

Security

Employees must identify themselves honestly, accurately and completely when setting up an NHSmail account.

Employees must ensure that passwords and answers to security questions for the NHSmail system are kept confidential and secure at all times. The local organisation administrator must be notified if there is any unauthorised access to an individual's NHSmail account.

NHS mail accounts must only be accessed from secure, encrypted devices that are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen. Employees accessing their NHSmail account from a non-NHS device (such as a home computer, personally owned laptop or smartphone) should do so via the web at www.nhs.net. Any access to NHS net accounts must only take place when the screen cannot be overlooked by members of the public or patients, service users. Care should be taken when opening emails which contain sensitive data to ensure privacy.

No virus or any other computer programme that may cause damage to NHS computers or systems should be introduced or forwarded. Anyone found to be deliberately responsible for introducing or forwarding a programme that causes any loss of service may be subject to proceedings for financial reparation.

Email messages can be a source of viruses that often sit within attached documents. Email attachments from unknown sources must be left unopened. Links in emails from unknown sources must not be opened. Any email which is thought to be suspicious should be reported to NHS mail helpdesk team by attaching the document to a new email and sending to spamreports@nhs.net. Further details of how to do this and for other cybersecurity information can be found at:

<https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/cybersecurityguide.pdf>

Professional Use of Email

All communication sent through the NHSmail service is assumed to be official correspondence from employees acting in their job role on behalf of the employing organisation. When, by exception, any communication of a



personal nature is sent the employee must clearly state that the message is a personal message and not sent in an official capacity.

Employees must familiarise themselves with the NHSmail training and guidance information available from the NHSmail website. (<https://portal.nhs.net/Help/policyandguidance>)

Care must be taken not to use the NHSmail service to harass other users or groups by sending persistent and/or inappropriate emails to individuals or distribution lists. Chain emails or other frivolous material should not be distributed or forwarded to individuals or distribution lists.

Emails should be considered the equivalent of sending a letter on THGPCG headed notepaper. The content of the email should be succinct and polite, consider whether issues that are complex and potentially contentious would be better managed via a conversation or a face to face meeting. Editing emails reflects a clarity in the communication, leads to fewer misunderstandings and is more likely to be read by the recipient.

Appendix One shows the THGPCG format for signatures and should be used by all staff.

Other Responsibilities

Employees must not use the NHSmail service in violation of any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is usually grounds for immediate dismissal and any illegal activity will be reported to the police. Use of the service for illegal activity will result in the immediate suspension of the NHSmail account.

Employees must not use the NHSmail service for personal commercial gain. This includes, but is not limited to: unsolicited marketing, advertising and selling goods or services.

Employees must not attempt to interfere with the technical components, both hardware and software, of the NHSmail system in any way. Employees must not use the NHSmail service to disable or overload any computer system or network. Where excessive account activity is detected the account may be suspended without notice to safeguard the service for all other users.

Employees must not attempt to disguise their identity or sending address.

Material that could cause distress or offence to another user must not be sent by NHSmail. This includes any material that that may be considered obscene, sexually explicit or pornographic.

Responsibilities when using the NHS directory service

It is the individual users responsibility to make sure that their details in the NHS Directory are correct and up to date.

It is the responsibility of the user to ensure that the addressee is the intended recipient. When sending personal information, the addressee should be double checked.

The NHS Directory must not be used for identifying individuals or groups of individuals to target for personal commercial gain.

Information Governance

Personal information held in an NHS net account is accessible to the data subject under Data Protection legislation. Emails should be treated like any other clinical or sensitive communication and care should be taken to ensure that content is accurate and the tone is appropriate. Email is admissible as evidence in a court of law and messages can be classified as legal documents.

Any relevant clinical data contained in emails should be attached to the patient record immediately and not stored in the NHSmail system.

NHSmail supports the secure exchange of information and is not designed as a document management system. Documents that are required for retention/compliance purposes should be stored in the usual Care

Group document management system in accordance with local Information Governance policies. Emails can be saved by using the 'File' tab in the Outlook system.

Caldicott and local Information Governance principles should apply whenever information is exchanged. Emails must be deleted as soon as no longer required and all emails (including those in the sent items and deleted items folders) must be deleted from the email system before six months after the date of the communication.

The NHSmail service is a secure service, which means that NHSmail is authorised for sending sensitive information, such as clinical data, between NHSmail and:

- NHSmail addresses (from an '*.nhs.net' account to an '*.nhs.net' account).
- Government secure email domains (between *.nhs.net and *.gsi.gov.uk, *.gse.gov.uk or *.gsx.gov.uk).
- Police National Network/Criminal Justice Services secure email domains (between *.nhs.net and *.pnn.police.uk, *.scn.gov.uk, or *.cjsm.net).
- Ministry of Defence secure email domains (between *.nhs.net and *.mod.uk).
- Local Government/Social Services secure email domains (between *.nhs.net and *.gcsx.gov.uk).
- The Health and Social Care Information Centre (*.hscic.gov.uk).

The NHSmail service includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services e.g. nhs.uk (*.secure.nhs.uk is considered secure), gmail, Hotmail. The following document provides information of how and when to use the encryption feature.



encryptionguide NHS
Mail.pdf

If sensitive information is to be exchanged the following guidelines should be followed:

- Any exchange of sensitive information must only be done as part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated.
- As with printed information, care must be taken that sensitive or personal information is not left anywhere that it can be accessed by other people (such as on a public computer without password protection).
- When sending sensitive information a delivery and read receipt should always be requested to ensure the information has been received safely. This is especially important for time-sensitive information such as referrals.
- Sensitive or personal data about a patient must not be held in the calendar if this can be accessed by other people who are not involved in the care of that person.
- If personal identifiable information is accessible to other people it is the individual users responsibility to make sure that those people have a valid relationship with the person.
- NHSmail must only be used for patient referrals if Choose and Book is not available.
- Personal information is accessible to the data subject, such as the patient, under Data Protection legislation.



The Care Group is entitled to seek access to the contents of any employee's mailbox, sent/received messages or other audit data as required to support information governance processes. This may be done without prior consent. Such requests are strictly regulated and the process is detailed in the NHSmail guidance.

Further information and guidance is available from NHS Digital and can be accessed via the following link <http://support.nhs.net/policyandguidance>

Appendix One

(Name) (relevant qualifications)

(Job Title)

(Service eg Health Visiting)

Tower Hamlets GP Care Group

Email:

Telephone No:



Equality Impact Assessment Tool for this Policy

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval

Policy Name: Email Usage Policy

Name of Assessor: Ruth Walters

		Yes/No/Possible/Not Applicable	Comments
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	Race	No	
	Religion or belief	No	
	Disability – learning disabilities, physical disability, sensory impairment and mental health problems	Possible	For those with a hearing impairment email communication may be preferable to verbal communication whether face to face or over the telephone.
	Gender	No	
	Sexual Orientation	No	
	Age	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	No	
4.	Is the impact of the policy/guidance likely to be negative?	No	
5.	If so can the impact be avoided?	No	
6.	What alternatives are there to achieving	No	

	the policy/guidance without the impact?		
7.	Can we reduce the impact by taking different action?	No	