Lindsey Lodge Hospice and Healthcare

EMAIL USE POLICY

Contents:

1 Scope

The purpose of the e-mail policy is to ensure the appropriate and effective use of e-mail on the F4 IT (F4 provide IT services to Lindsey Lodge) systems by:

- Setting out the rules governing the sending, receiving and storing of e-mail.
- Establishing Lindsey Lodge and user rights and responsibilities for the use of the system.
- Promoting adherence to current legal requirements and NHS information governance standards.

This e-mail policy applies to the following areas:

- The use of NHS e-mail accounts.

2 Introduction

E-mail is an increasingly popular form of communication. It can be of great benefit to the organisation when used appropriately but its use also exposes Lindsey Lodge to new risks. These include non-compliance with various statutory requirements for example, data protection legislation, threats to IT security and ineffective communication.

3 Definitions

For the purposes of this policy, e-mail includes the e-mail accessed via NHS Mail.

4 Roles & Responsibilities

Users will be required to read the Acceptable Use Policy and sign a declaration that they have understood it and agree to abide by its content prior to receiving access to NHSmail. This is their commitment to all NHSmail users and the public that they will be mindful of the importance of the information that they share over NHSmail.

Failure to comply with this policy and procedures may have serious consequences for the individual including civil, criminal and/or action being taken in accordance with the Lindsey Lodge disciplinary procedure.

5 The Procedure

5.1 Confidentiality

Confidential, sensitive and Patient identifiable information should only be sent via email when absolutely necessary. The NHS mail service is a secure service, this means that NHS mail is authorised for sending sensitive information, such as clinical data, between NHS mail and:

- NHS mail addresses (i.e. from an '*.nhs.net' account to an '*.nhs.net' account)
- Government secure email domains (between *.nhs.net and *.gsi.gov.uk, *.gse.gov.uk and *.gsx.gov.uk)
- Police National Network/Criminal Justice Services secure email domains (between *.nhs.net and *.pnn.police.uk, *.scn.gov.uk, *.cjsm.net)
- Ministry of Defence secure email domains (*.nhs.net and *.mod.uk)
- Local Government/Social Services secure email domains (*.nhs.net and *.gcsx.gov.uk)

Whenever you send sensitive or patient identifiable information to an address outside of NHS Mail you must use the NHS encryption tool. This includes addresses that end in @nhs.uk as not all of these conform to the secure mail standard. Mail can be sent by adding the word **{secure}** including the square brackets, to the start of the subject line of the email.

Where staff are contacted by service users or relatives in relation to their care, they should always respond to them in the first instance via the encryption tool. Please refer to F4 IT for guidance on how to use this.

If you intend to use the service to exchange sensitive information you should adhere to the following guidelines:

- You should make sure that any exchange of sensitive information is 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.

- Caldicott and local Information Governance principles should apply whenever sensitive information is exchanged.

- As with printed information, care should be taken that sensitive or personal information is not left anywhere that it can be accessed by other people, e.g. on a public computer without password protection.

- When you are sending sensitive information you should always request a delivery and read receipt so that you can be sure the information has been received safely. This is especially important for time-sensitive information.

- You must not hold sensitive or personal data in your calendar if your calendar may be accessed by other people who are not involved in the care of that person.

- If personal identifiable information is visible to other people it is your responsibility to make sure that those people have a valid relationship with the person.

- You must always be sure that you have the correct contact details for the person (or group) that you are sending the information to. This is especially important if you are sending information using the SMS services. If in doubt you should check the contact details in the NHS Directory.

- If it is likely that you may be sent personal and/or sensitive information you must make sure that the data is protected. You should only access your account from secure, encrypted devices which 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.

- Remember that personal information is accessible to the data subject i.e. the patient, under Data Protection legislation.
- Where practical remove identifiers such as client/patient name, date of birth etc, and phone the recipient with key to identification.
- Use only the minimum necessary information think about previous information contained in the 'email chain'; do not repeat this information unless needed.
- Mark the email subject heading as 'personal information'. You may wish to add a number/code to aid your tracking of emails and replies. Do not use the patients/client's name in the subject heading.
- When replying to an email containing personal information, do not use the 'reply all' button unless absolutely necessary.
- Where the client/patient is identified in the email (sent or received emails) save in the client/patient personal record (both manual and electronic records) and delete emails from your system at the earliest opportunity.
- Include a disclaimer, as detailed in section 5.3.
- Ensure that plans are in place for your emails to be dealt with in your absence. However note that the use of the auto-forward facility is not allowed.
- If you receive an email in breach of this guidance follow your local incident reporting system as detailed in the Data Protection Management Policy.

5.2 Monitoring

Staff are advised that in accordance with the Employment Practices Code monitoring of E-mail traffic will take place subject to the following guidance:

- Monitoring is required to ensure that employees do not breach any regulations (such as those on harassment and discrimination) which could have a legal impact on Lindsey Lodge
- Spot checks will be done as opposed to continuous monitoring.
- Traffic will be monitored as opposed to content unless there are reasons for checking specific e-mails.

Inappropriate use of the e-mail may result in the facility being withdrawn and may lead to action being taken in accordance with the Lindsey Lodge disciplinary procedure.

5.3 Disclaimers

Messages of a confidential nature should include the following disclaimer:

The contents of this email are not necessarily the policy or opinion of Lindsey Lodge or any person employed by it. This transmission is intended only for the named recipient(s) and is confidential in nature. If received in error, please return it to the sender and destroy any copies immediately.

5.4 Bandwidth

This is the term that is used to describe the amount of information that can be transmitted on a network over a given time. Individual users sending very large files such as videos if sending to large numbers of addressees can have an adverse effect on the availability of the network for other users. To avoid this, users should be aware of the problem and where possible avoid sending large e-mails with attachments. Text should be included in the body of the message as opposed to attaching a Word document, and where a file can be located on the network or Intranet the location should be given rather than copying the file. This is particularly important for multiple addresses.

5.5 Mailbox Size

Due to the number of users on the system, it is a key requirement that users have a set limit set in terms of the size of their mailbox. These limits may change over time subject to technical storage issues. Users will receive a notification when their mailbox is reaching the limit. A further message will be sent when the mailbox reached the limit and at this point users may be blocked from sending any further items until they reduce the size of their mailbox. This can be done either by deleting items no longer required or archiving folders onto the network storage. F4 IT service desk can be contacted for assistance in resolving mailbox size issues.

6 Inappropriate Use of E-mail

The use of e-mail in the following types of activities is specifically prohibited:

- Illegal, fraudulent, or malicious activities.
- Partisan political activity, political or religious lobbying.
- Advocacy or activities on behalf of organisations having no connection with Lindsey Lodge
- Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitations of business or services, sales of personal property.
- Unauthorised fund-raising or similar activities, whether for commercial, personal or charitable purposes.
- Distributing offensive or obscene material such as pornography and hate literature.
- Annoying or harassing another person, e.g. by sending or displaying uninvited e-mail of a personal nature; joke emails or by using lewd or offensive language in an e-mail message.
- Using another person's account or identity without his or her explicit permission, e.g. by forging e-mail.
- Viewing, damaging, or deleting files or communications belonging to others without appropriate authorisation or permission.
- Attempting to circumvent or defeat security or auditing systems without prior authorisation and other than as part of legitimate system testing or security research.
- Activities which may bring Lindsey Lodge into disrepute.

These, and other inappropriate activities, may result in action being taken in accordance with the Lindsey Lodge disciplinary procedure against the person found misusing the e-mail service for such purposes.

6.1 Management of E-mail

All email messages are subject to Data Protection Legislation and can also form part of the corporate record. Staff should also be aware that email messages could be used as evidence in legal proceedings.

There may be occasions when it is necessary to access email messages from an individual's mailbox when a person is away from the office for an extended period, for example holiday or sickness. Users should be aware that e-mail accounts can be accessed if an organisational need is determined. The reasons for accessing an individual's mailbox are to action:

- Subject access request under the Data Protection Act.
- Evidence in legal proceedings.
- Evidence in a criminal investigation.
- Line of business enquiry.
- Evidence in support of disciplinary action.

Where it is not possible to ask the permission from the member of staff whose mailbox needs to be accessed, the procedure for gaining access their mailbox is:

- Gain authorisation from the Chief Executive.
- Submit a request to F4 IT Support Desk on 01472 256789.
- Request must be authorised by the individual`s line manager.
- A record is made of the reasons for accessing the mailbox together with the names of the people who were present.
- Inform the person whose mailbox was accessed at the earliest opportunity.

It is less likely that this procedure will need to be followed if email records are managed appropriately or mailbox access has been delegated to a trusted third party.

6.2 Good Practice and Effective Use of Email

The following guidelines have been included into this policy document to provide assistance to users in the effective use of Email services.

Subject Line.

- Ensure the subject line gives a clear indication of the content of the message.
- Indicate if the subject matter is sensitive.
- Use flags to indicate whether the message is of high or low importance and the speed with which an action is required.
- Indicate whether an action is required or whether the email is for information only.

Subject and Tone.

- Greet people by name at the beginning of an email message.
- Identify yourself at the beginning of the message when contacting someone for the first time.
- Ensure that the purpose and content of the email message is clearly explained.
- Include a signature with your own contact details.
- Ensure that the email is polite and courteous and appropriately worded.
- Tone of an email message should match the intended outcome.

Make a clear distinction between fact and opinion

- Proof read messages before they are sent to check for errors.
- Include the original email message when sending a reply to provide a context.
- Where the subject of a string of email messages has significantly changed start new email message, copying relevant sections from the previous string of email messages.
- Ensure email messages are not unnecessarily long.
- Ensure that attachments are no longer versions of emails.
- Summarise the content of attachments in the main body of the email message.

Structure and Grammar

- Try to use plain English.
- Check the spelling within the email message before sending.
- Use paragraphs to structure information.
- Put important information at the beginning of the email message.
- Take care when using abbreviations.
- Avoid using CAPITALS.
- Try not to over-use bold and coloured text.

Addressing

- Distribute email message only to the people who need to know the information.
- Using 'reply all' will send the reply to everyone included in the original email. Think carefully before using 'reply all' as it is unlikely that everyone included will need to know your reply.
- Use the 'To' field for people who are required to take further action and the 'cc' field for people who are included for information only.
- Consider if BCC should be used to ensure email addresses are kept private
- Think carefully about who should be included in the 'cc' field.
- Ensure the email message is correctly addressed.

6.3 Emailing Sensitive and Patient Identifiable Information

When emails are sent between NHSmail users, they are always encrypted, which means that you can be sure that the information you send is safe and cannot be intercepted. When you send an email to a user outside of NHSmail this security is not always guaranteed.

The NHSmail Encryption Tool is a service that works out if the recipient is using a government accredited secure email address. If they are, it sends the email as normal. Otherwise, it places the contents of the email on a secure website instead, and sends the recipient a link to access the email.

When Should I Use It?

Whenever you send sensitive or patient identifiable information to an address **outside** of NHSmail. This **includes** addresses that end in **@nhs.uk** as not all of these conform to the secure email standard.

Patient identifiable data includes:

- Patient's name, address, full post code, date of birth
- Pictures, photographs, videos, audio-tapes or other images of patients
- NHS number and local patient identifiable codes e.g. hospital number

- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified

Sensitive information includes:

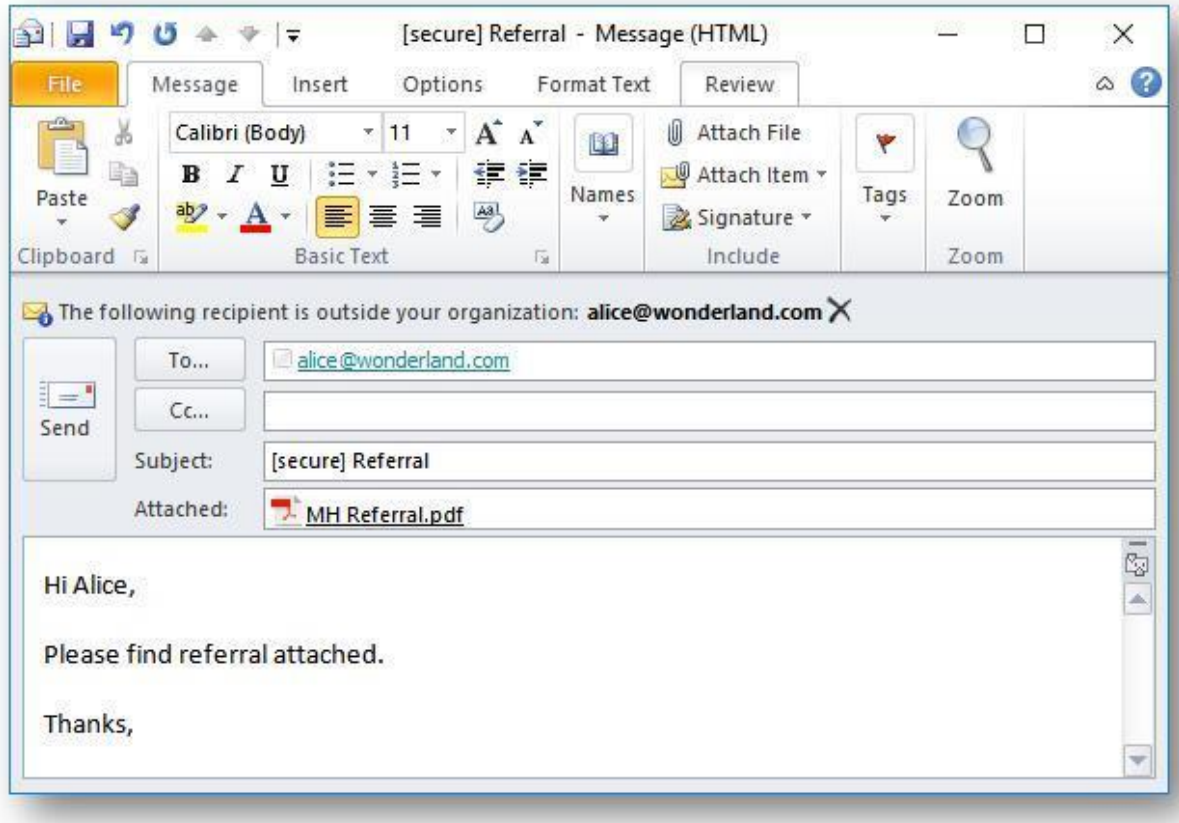
- Patient/service user information
- Racial/ethnic origin
- Religious beliefs
- Criminal offences/proceedings
- Commercially confidential information

If you are sending to NHSmail accounts (ending in **@nhs.net**) then there is no need to use the encryption tool, although NHSmail will just ignore and send the email as normal anyway.

Recently the local authorities have joined the secure email standard, so you can safely send sensitive and patient identifiable information directly to **@nelincs.gov.uk** and **@northlincs.gov.uk** addresses without using the tool.

How Do I Use It?

Sending Secure Emails
Add the word **[secure],** including the square brackets, to the start of the subject line of the email e.g.:



Further information can be found in the NHSmail encryption guidance for senders
Receiving Secure Emails

If the recipient is using an email address that is not securely connected to NHSmail, then it will send the recipient a link to a website where they can view the email and any attachments. The first time the user gets one of these emails they will need to register with the website and set up a username and password.

Details on how to do this can be found in the NHSmail encryption guidance for recipients
It may be useful to send this link to the recipient in a normal email before sending them the secure information.

7 Associated Policies

- *Acceptable Internet Use Policy*
- *Records management Policy*
- *Information Security Policy*
- *Confidentiality & Data Protection Policy*
- *Social Media*

8 Consultation

IT & IG committee

9 Dissemination

Via Lindsey Lodge `L` drive policies/guidelines of this form.

10 Equality Act

10.1 In accordance with the Equality Act (2010), Lindsey Lodge will make reasonable adjustments in the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage. The Hospice will endeavour to develop an environment within which individuals feel able to disclose any disability or concern which may have a long term ad substantial effect on their ability to carry out their normal day to day activities.

10.2 Lindsey Lodge will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Hospice's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010).

REFERENCES: F4 IT, NHS Mail Policy				
Lead Author of Policy: Kay Fowler, IT Support Officer **Responsible Sub-group** IT & IG committee **RATIFICATION DATE BY TRUSTEES 19th October 2017** Review interval 3 year				
TO BE REVIEWED	REVIEW COMPLETED	BY	APPROVED BY	CIRCULATION
Oct 2020	Mar 21	Kay Fowler	IT & IG	Via team talk
Mar 2024				