



Yorkshire and the Humber

Yorkshire and the Humber Strategic Health Authority

Email Policy

Policy Reference Information

Policy name	Email policy
Version	1.3
Status	Draft
Originator/Author	Stephen Rose (Health Informatics Service)/Trevor Parsons (NPfIT)
Responsible Director	Director of Finance & Investment (SIRO)
Approved by	
Date Issued	
Last review date	n/a
Next review date	March 2011
Applies to	All SHA staff (including hosted organisations/programmes)

Document Revision Record

Version	Description of Change	Reason for Change	Author	Date

Contents

		Page No
1	Introduction	1
2	Objective	1
3	Email and the Law	1
4	SHA Responsibilities	2
5	Access to the Email System	2
6	Sensitive Personal Information	3
7	Best Practices	4
8	Personal Use	5
9	Computer Virus Infection	5
10	System Monitoring	5
11	Email Accounts	6
12	Training	6
13	Questions	6
14	Legal References	7
15	Associated Documents	7
Appendix A	Definitions	8
Appendix B	Freedom of Information	11
Appendix C	Password protecting a Word document	12
	Password protecting an Excel document	13

1 INTRODUCTION

1.1 This document defines the Email Policy for Yorkshire and the Humber Strategic Health Authority (referred to hereafter as the SHA). This policy is adhered to and supported by the Health Informatics Service (THIS) who provide IT support for and are hosted by Calderdale and Huddersfield NHS Foundation Trust. The Email Policy applies to all business functions and information contained within the email system. This document:

- a) sets out the SHA's policy for the protection of the confidentiality of information and the integrity and availability of the email system;
- b) establishes SHA and User responsibilities for the email system;
- c) provides reference to documentation relevant to this policy.

1.2 The purpose of this policy is to ensure the proper use of the SHA's email system and to make users aware of what the SHA deems as acceptable and unacceptable use of its email system.

1.3 If there is evidence that any user is not adhering to this policy, they maybe dealt with under the SHA's Disciplinary Procedure.

2 OBJECTIVE

2.1 The objective of this policy is to ensure the security of the SHA's email system. The SHA will:

- a) Ensure Availability
Ensure that the email system is available for users;
- b) Preserve Integrity
Protect the email system from unauthorised or accidental modification of the SHA's information;
- c) Preserve Confidentiality
Protect the SHA's information against unauthorised disclosure.

3 EMAIL AND THE LAW

3.1 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, by following this policy the email user can minimise the legal risks involved in the use of email.

Breach of this policy may be classed as gross misconduct under the SHA's Disciplinary procedure.

- a) You must not send emails with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic or homophobic remarks or

depictions. If you receive an email of this nature you must promptly notify your line manager, who will instigate an incident report and investigation.

- b) You must not forward emails with any libellous, defamatory, offensive, harassing, racist, obscene homophobic or pornographic remarks or depictions as you and the SHA can be held liable. If you receive an email of this nature, you must promptly notify your line manager who will instigate an incident report and investigation.
- c) You must not forward a confidential message without acquiring permission from the sender first;
- d) You must not intentionally/knowingly send an attachment that contains a virus as you and the SHA can be held liable;
- e) You must not send unsolicited email messages (see Appendix A for definition of 'unsolicited' email);
- f) You must not forge or attempt to forge email messages;
- g) You must not send email messages using another person's email account except if access has been granted by proxy e.g. in the case of a manager and PA;
- h) You must not knowingly breach copyright or licensing laws when composing or forwarding emails and email attachments. (See Appendix A for definitions.)

4 SHA RESPONSIBILITIES

- 4.1 The SHA will ensure that all users are properly trained before using the email system.
- 4.2 The SHA will take all reasonable steps to ensure that users of the email service are aware of policies, protocols, procedures and legal obligations relating to the use of email. This will be done through training and staff communications at departmental and SHA-wide levels.

5 ACCESS TO THE EMAIL SYSTEM

- 5.1 Authorised access to the email system is obtained by applying to the IT Service Desk.
- 5.2 Users will be sent a Code of Connection agreement as required, and must familiarise themselves with the associated policies.
- 5.3 Users are responsible for ensuring unauthorised users do not use their email account.

- 5.4 The SHA reserves the right to manage a mailbox on behalf of an individual i.e. view, archive and delete items, as appropriate. This must be authorised by an appropriate line manager.
- 5.5 The SHA reserves the right on occasions to grant access to a user's mailbox to a different member of staff. This will be in the event of unplanned absence or prolonged periods of sick leave and must be authorised in advance by an appropriate line manager.

6 SENSITIVE PERSONAL INFORMATION

- 6.1 For a definition of 'person identifiable and sensitive information' see Appendix A.
- 6.2 Wherever possible person identifiable data should be anonymised.
- 6.3 Email sent within the SHA (i.e. from a yorksandhumber.nhs.uk email address) can be treated as secure as it is within a secure network. However, care must be taken at all times to ensure any e-mail is correctly addressed and is sent only to the intended recipient/s. Person identifiable and sensitive information can be contained within or attached to internal emails without further protection. Nevertheless if the data is particularly sensitive or contains data about a number of individuals, encryption or password protection of an attachment would provide additional security. Care must be taken not to forward any such emails inappropriately.
- 6.4 Person identifiable information relating to patients or staff (e.g. health, employment or financial details) or commercially sensitive information must not be sent outside of the organisation by email unless it is encrypted to the NHS standards using software approved by the SHA. Your general mail account set up by the SHA does not yet support encrypted technologies by default (*meaning of encrypted – the practice of encoding data in order to prevent any but the intended recipient from reading it*). Therefore person identifiable or sensitive information should be sent in an encrypted attachment.
- 6.5 As an alternative to using an SHA email account, person identifiable data can be sent from one nhs.net email account to another. This is encrypted in transit but offers no protection against sending the information to the wrong address or what happens to the information at its destination. Another alternative suitable for larger files or data sets is the Secure File Transfer Service.
- 6.6 In exceptional circumstances only, it may be permissible, with prior approval by the SHA Caldicott Guardian, to send sensitive or person identifiable information as a password protected attachment and the password sent by another route, such as text to a mobile phone. (See guidance on password protection in Appendix A). Where this applies, staff should contact the Confidentiality and IM&T Security Officer in the first instance in relation to the use of email for transmitting sensitive person identifiable information.

- 6.7 Do not store details in your electronic diary containing person identifiable information or other confidential staff information.

7 BEST PRACTICES

- 7.1 The SHA considers email as an important means of communications and recognises the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Therefore, the SHA wishes to encourage users to adhere to the following guidelines:

- a) Write well structured emails;
- b) Include your name, job title and SHA name;
- c) Include the standard disclaimer:

This is an e-mail from Yorkshire and the Humber Strategic Health Authority. The message and any files transmitted with it are confidential. If you are not the intended recipient, any reading, printing, storage, disclosure, copying or any other action taken in respect of the email is prohibited and may be unlawful. If you have received this message in error, please notify the sender immediately by using the reply function and then delete what you have received. The SHA accepts no responsibility for any changes to this message after it has been sent by its original author. The views or opinions contained herein do not necessarily represent the views of Yorkshire and the Humber SHA. The email or any of its attachments may contain data that falls within the scope of the Data Protection Act and the Freedom of Information Act. You must ensure that any handling or processing of such data by you is fully compliant with the terms and provisions of the Data Protection Act 1998 and Freedom of Information Act, 2000.

- d) Give the e-mail a title
- e) Use the spell checker before you send out an email;
- f) Do not print emails unless you really need to for work purposes. Emails can be saved, if you need to keep them;
- g) If you need a reply to your email by a particular date let the recipient know this;
- h) If you forward emails, state clearly what action you expect the recipient to take;
- i) Only mark emails as important if they really are important;
- j) Ensure you only send emails that are essential. Send your email only to people who need to see it. Do not send emails to all in your address book as this can unnecessarily block the system;
- k) Delete any email messages that you do not need to keep (taking into consideration (j) below) and maintain your mailbox within its allowed limits.

- l) Remember that emails can be requested under the Freedom of Information Act. Store any emails containing information likely to be requested (e.g. spending of public money, development of services) in a separate folder to allow easy and efficient retrieval (see Appendix B for further list of examples).

8 PERSONAL USE

8.1 Although the SHA's email system is meant for business use, the SHA allows the reasonable use of email for personal use if certain guidelines are adhered to:

- a) Personal use of email should not interfere with work;
- b) Personal emails must also adhere to the guidelines in this policy;
- c) Personal emails should be kept in a separate folder, named 'Private'. The emails in this folder must be deleted on a regular basis so as not to clog up the system. In appropriate circumstances where the SHA feels that this policy has not been complied with it reserves the right to look at this folder.
- d) The forwarding of chain letters, junk mail and executables is forbidden. The sending of unsolicited mail is considered by many users as wasteful of user time and can also disrupt the service for other users and is forbidden;

9 COMPUTER VIRUS INFECTION

9.1 If you suspect that you have received a virus by email - inform the IT Service Desk.

Do not attempt to remove the virus yourself. The IT Service Desk will need to know what virus it is:

- a) Do not switch off your PC unless told to do so by the IT Service Desk;
- b) Where you suspect the presence of a virus do not send any further emails until the IT Service Desk have confirmed that it is safe to do so.

10 SYSTEM MONITORING

10.1 All emails including personal emails are automatically monitored for viruses and to maintain the size of accounts. All email traffic (incoming and outgoing) are logged automatically. These logs are audited periodically.

10.2 The content of emails is not routinely monitored. However, the SHA reserves the right to inspect, monitor and retain message content as required to meet legal, statutory and business obligations.

10.3 If there is evidence that you are not adhering to the guidelines set out in this policy, this will be dealt with under the SHA Disciplinary Procedure.

11 EMAIL ACCOUNTS

11.1 All email accounts and email content maintained on SHA email systems are the property of the SHA.

12 TRAINING

12.1 If you require user training in basic computer skills or the use of email please contact the Health Informatics Training Service on 0845 1272600

13 QUESTIONS

13.1 If you have any questions or comments about this Email Policy, please contact the Confidentiality and IM&T Security Officer on 0845 1272600.

13.2 If you do not have any questions the SHA presumes that you understand and are aware of the rules and guidelines in this Email Policy and will adhere to them.

14

LEGAL REFERENCES

Copyright, Designs & Patents Act 1988
Access to Health Records Act 1990
Computer Misuse Act 1990
The Data Protection Act 1998
The Human Rights Act 1998
Electronic Communications Act 2000
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Environmental Information Regulations 2004
Health & Social Care Act 2011

15

ASSOCIATED DOCUMENTS

(Policies, protocols and procedures)

Internet Policy
Standards of Conduct for SHA Staff
Disciplinary Procedure
Confidentiality Policy Statement and Guidance
Information Governance Policy and Strategy
Incident Reporting Procedure
Policy and Procedure for Responding to Freedom of Information Act Requests

1 DEFINITIONS

1.1 Defamation and Libel

What is defamation?

A published (spoken or written) statement or series of statements, which affects the reputation of a person or an organisation and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss.

DO NOT

Make statements about people or organisations in any email that you write without verifying their basis in fact. You must not forward any emails that may be defamatory.

1.2 Harassment

What is harassment?

Any unwarranted behaviour, which is unreasonable, unwelcome or offensive. This may include physical contact, comments or printed material, which causes the recipient to feel threatened, humiliated or patronised.

Harassment takes many forms. It can range from extreme forms such as violence and bullying, to less obvious actions like ignoring someone at work. Whatever the form, it will be unwanted behaviour that is perceived as unwelcome and unpleasant by the recipient. Harassment can be on a variety of grounds, including sex/gender, race, sexual orientation, mental status, age, physical/mental disability. Note that this list is not exhaustive.

DO NOT

Use email to harass other members of staff by sending messages that they consider offensive or threatening.

1.3 Pornography

What is pornography?

Pornography can take many forms. For example, textual descriptions, still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography that is legal in the UK may be considered illegal elsewhere. Because of the global nature of email these issues must be taken into consideration. Therefore, the SHA defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The SHA will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence.

See also section 1.3 in Appendix A of the Internet Policy which gives guidance for managers on the discovery of indecent images of children on computer.

DO NOT

- Send, deliberately view or forward emails containing pornography. If you receive an email containing pornography you should report it to the IT Service Desk or your line manager.
- Send, deliberately view or forward emails with attachments containing pornography. If you receive an email with an attachment containing pornography you should report it to the IT Service Desk or your line manager.
- Save pornography material that has been transmitted to you by email.

What are the consequences of not following this policy?

- Users and/or the SHA can be prosecuted or held liable for transmitting or downloading pornographic material, in the UK and elsewhere.
- The reputation of the SHA will be seriously compromised if its systems have been used to access or transmit pornographic material and this becomes publicly known.
- Users found to be in possession of pornographic material, or to have transmitted pornographic material, will be dealt with under the SHA's Disciplinary Procedure.
- This may constitute gross misconduct under the SHA's disciplinary procedure.

1.4 Copyright

What is copyright?

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. So a lack of the symbol does not indicate a lack of copyright. In the case of SHA standard use of computer software, the SHA purchases licences on behalf of its users.

DO NOT

- Alter any software programs, graphics, etc without the express permission of the owner.
- Claim someone else's work is your own.
- Send copyrighted material by email without the permission of the owner. This is considered copying.

1.5 Unsolicited Email

What is unsolicited email?

Electronic mail which is unrequested by the recipient and is of an advertising, promotional (including virus notifications) or humorous nature

1.6 Defining Person Identifiable and Sensitive Information

“Person identifiable information” relates to information about a person which would enable that person’s identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. “Sensitive information” can be broadly defined as that which if lost, misdirected or compromised could affect individuals, organisations or the wider community. This is wider than, but includes, data defined as sensitive under the Data Protection Act 1998, for example, financial and security information about an organisation is likely to be deemed “sensitive”, as are an individual’s bank account details. The Data Protection Act 1998 refers to ‘sensitive personal data’ as including all information about physical or mental health or condition, or sexual life.

FREEDOM OF INFORMATION

The following is a list of examples of types of information which may be requested under the Freedom of Information Act 2000, but it is by no means an exhaustive list;

- Financial information
- Correspondence relating to the business of the SHA
- Briefing provided to or by the SHA
- Decisions taken about strategies and associated correspondence
- Briefing papers
- Contractual information
- Reports, policies, procedures and guidance

PASSWORD PROTECTING A MICROSOFT WORD DOCUMENT

(Instructions for users of Microsoft Word 2000 or later versions)

With the Word Document open

Click: **File menu**

Select: **Save As**

Select where to save the document

Type in a File name

In the **Save as Type** box check the document will be saved as a Word Document

Click: The black arrow to the right of Tools menu on the [Save As] box.

Select: **Security Options**

The Security dialog box opens

Type a password in the [Password to Open] box (it will appear as asterisks/stars)

Click: **Ok**

Confirm your password when prompted in the confirm password dialog box

Click: **Ok**

Click: **Save** on the Save As Dialog Box

Close the Document

To Open the Document

Click: **File menu**

Select: **Open**

Navigate to your shared Drive or wherever you saved the document

Double click onto the File to open it

The Password box opens on screen

Enter your password

Click: **Ok**

PASSWORD PROTECTING A MICROSOFT EXCEL DOCUMENT

Once you have completed your document, left click on the 'tools' menu and then select 'Options' from the drop down menu.

On the menu that appears left click on the 'Security' tab and enter a password in the 'Password to Open' box. Doing this prevents anyone from being able to open the document without the password you assign.

Click on OK once you have chosen a password. A new window will appear asking you to verify the password you have chosen. Once you have done this save the document as normal.

If you lose or forget the password, it cannot be recovered. It is therefore advisable to keep a list of passwords and their corresponding workbook and sheet names in a secure place. Passwords are case sensitive.

The file can be opened in the normal way; a dialogue box will come up requiring the entry of the password chosen by the person who created the file. Enter the password and click OK to open the file.

4 FURTHER INFORMATION

If you would like any further information please do not hesitate to contact the Confidentiality and IM&T Security Officer on 0845 1272600.