NHS
East of England Ambulance Service
NHS Trust

Electronic Communications Policy

Document Reference	POL046
Document Status	Approved
Version:	4.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
IM&T	15/10/19	IT Security & Resilience Manager
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
Draft V3.1	11 November 2021	Presented to and approved at IGG
V4.0	13 December2021	Approved by Compliance and Risk Group

Document Reference	POL046 Directorate: IM&T
Recommended at Date	Information Governance Group 11 November 2021
Approved at Date	Compliance and Risk Group 13 December 2021
Valid Until Date	December 2023
Equality Analysis	Completed and attached
Linked procedural documents	None
Dissemination requirements	All staff via East24
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

1. Introduction

1.1 This Policy sets out Trust's position with regard to the use of electronic communications. This Policy applies to all staff at East of England Ambulance Service NHS Trust including staff who may not be directly employed by Trust (e.g. volunteers, agency staff, contractors, self-employed consultants).

1.2 This policy applies to all equipment owned and solutions provided by the Trust which is capable of electronic communications, including but not limited to, desktop PC's, laptops, PDA's and Smartphones; and covers all forms of electronic communications including but not limited to e-mail, SMS, Teams and electronic system generated messages.

1.3 This policy does not cover the use of social media, that is governed by the Social Media and Digital Policy.

2. Purpose

2.1 The purpose of this Policy is to ensure that electronic communications solutions are used in an appropriate way, and to make staff aware of what the Trust considers to be an acceptable use of these communications. This Policy also sets out how the use of electronic communications is monitored by Trust.

3. Policy Statement

3.1 Staff should usually only use electronic communications for work related purposes. This includes work related research or educational purposes.

3.2 Staff should only use electronic communications for their personal use in accordance with paragraph 4.1 below.

3.3 A failure to comply with this Policy may result in disciplinary action or access to this communication medium being denied.

3.4 If you are unclear about any aspect of this policy you must consult your manager. If you wish to use electronic communications and are unsure as to whether your proposed use falls within the Policy, seek permission from your manager.

4. Use of Electronic Communications (General)

4.1 Trust provides electronic communications solutions to its staff for work related purposes. These are not intended to be used for personal or private communications unrelated to work. However, social messages between work colleagues (e.g. to arrange to meet for lunch) are permitted provided they are kept brief and are not in any sense disruptive. Similarly, brief and necessary communications with family and friends are permissible.

4.2 Trade union representatives are entitled to use the electronic communications facilities for legitimate trade union business to communicate with members and full-time union officers. Staff may use electronic communications to communicate with their trade union officials.

4.3 Electronic communications must not be used to make defamatory or offensive comments including jokes and inappropriate remarks made at someone else's expense.

4.4 Video clips, graphics or executable files should not be sent using electronic communications unless related to the business of the Trust.

4.5 Electronic communications should be used instead of internal memos wherever possible.

4.6 Staff should think carefully about the contents of any electronic communications message before sending it. You should not say anything in electronic communications that you would not be prepared to say in hard print.

4.7 Be selective about who receives your electronic communications. Ask yourself who really needs to see this electronic communication ? In particular with e-mail, and for the same reason, use distribution lists and 'reply to all' with care.

4.8 Electronic communications should not be assumed to be confidential. They can be subject to disclosure if relevant to any legal proceedings / internal investigations. Do not send electronic communications on sensitive subjects without first checking with a senior member of staff.

4.9 If you are sending any electronic communication with an attachment, make sure you are sending the correct documents by opening and checking the attachment prior to sending it.

4.10 If you expect an urgent response from the recipient(s), do not assume they have opened and read the message. You should contact people by telephone to follow up your electronic communications if an urgent response is required.

4.11 Electronic communications can be an impersonal means of communication. You should never use electronic communications as a vehicle for communicating difficult messages – in such situations it is usually more appropriate to use the telephone or speak to the person directly. You should be aware that electronic communications can be used aggressively, in ways which bully or harass colleagues.

4.12 Staff must always use their Trust e-mail account, or their NHSMail account with an appropriate signature including the Trust name, for Trust business.

4.13 It is recommended that wherever possible all users check their mailbox at least twice a day (unless they are absent from the office or in meetings) and respond to requests promptly.

4.14 If you are away from the office for a period of time, you should activate the out of office feature to inform people you are away from the office, for how long, and who to contact in your absence. Also consider using the "delegate" feature available to allow someone else access to your mailbox if appropriate.

4.15 Automatic forwarding of emails from personal accounts will only be permitted in limited circumstances.

1) Setup of auto-forwarding using the "Start Forwarding" option has been permanently disabled for all staff, and anyone who had this set prior to the implementation of Office 365 has had it removed.

2) Using "Inbox Rules" to automatically forward emails to another @eastamb.nhs.uk or other secure mail domain: If an individual decides to setup an auto forward of emails they receive by creating an inbox rule that forwards to another member of staff within

eastamb.nhs.uk, these emails will be delivered. In the same vein, if it is to a secure mail domain such as nhs.net, it will also be delivered. These rules are the responsibility of the individual.

3) Using "Inbox Rules" to automatically forward emails to unsecure domains: If an individual sets an Inbox Rule to forward email to an unsecure domain, these emails will not be sent.

Automatic forwarding of emails at source is not permitted without authority from the IM&T Security and Resilience Manager, the Deputy Head of IM&T, the Head of Digital Delivery, the Head of Live Services or the Chief Information Officer . Requests for auto-forwarding should be made to the IT Service Desk stating your justification. Requests will be considered on a case by case basis.

4.16 When composing electronic communications use the same language as you would for a memo or letter and use the spell check facility before sending. Finally, when using e-mail, sign off with your name, organisation and telephone number.

5. Use of Electronic communications (Personal Data)

5.1 The use of email for exchange of personal data between Trust accounts (from eastamb to eastamb) and between eastamb and NHSMail is permitted.

5.2 Emails containing personal data can only be sent to external organisations that have a suitable accredited secure email domain and a secure end to end connector is in place between the Trust and the external organisation. A list of accredited domains is maintained

and held by IT and is available upon request, if a new connector is required staff should contact the IT Service Desk to arrange one t be put in place.

5.3 Responsibility rests with staff for ensuring personal data is only transmitted to appropriate recipients.

- Ensuring that the message is kept secure and confidential
- Checking they have used the correct address for the intended recipients before sending
- Ensuring Caldecott principles are followed regarding supplying only the minimum necessary information and access being on a strict need-to-know basis.
- The forwarding of personal data received via electronic communications is not permitted unless it follows the same guidelines shown above for the original transmission and is authorised by the original sender, either explicitly or as part of an agreed and documented work-flow process.

5.4 In the event of an individual requesting information about themselves via email, who supply an email address on a domain not on the approved list (Gmail, Yahoo, etc), staff must explain to them that any email sent to a personal account may be at risk and must get written permission from the individual stating they accept this risk.

6. Housekeeping

6.1 Delete all electronic communications messages once read or archive any messages required for later use. Staff should empty deleted items folders regularly. It is recommended to set Outlook to empty the deleted items folder on exiting.

6.2 Delete or archive all sent messages from sent items folders on a regular basis.

6.3 Folders should be used to organise those messages you wish to keep them. However, you should review your folders on a regular basis and delete all unwanted messages.

7. Security

7.1 Passwords on documents should only be used if you are involved with private and confidential work.

7.2 You must be alert to the possibility that electronic communications containing viruses may be sent to you. In no circumstances must you open an electronic communication or an attachment to an electronic communication that seems in any way suspicious without first checking with a member of the IM and T Directorate. Detailed guidance on electronic communications attachments may be sent to you from time to time and you must act in accordance with such guidance.

7.3 If you receive an electronic communications that appears to be 'spam' – part of a mass mailing that does not appear to be relevant and you do not recognise the sender – make a note of the sender's address and inform the IT Service Desk. Ensure that you delete the received electronic communications without opening any attachments.

8. Personal devices

Personal devices may be used to access Trust email accounts using in-built or 3rd party mail clients provided

staff accept that their devices will become enrolled in the Trust's Mobile Device Management solution, that policies will be enforced on their device by the Trust and that the Trust will have control over that device via the company portal.

Staff not wishing to accept the above will only be permitted access on their personal devices via a web browser.

9. Unacceptable Use of Electronic communications

The following are regarded by the Trust as unacceptable uses of electronic communications. The list of guidelines is not exhaustive and the Trust may from time to time treat other actions or conduct as constituting a breach of the spirit of this Policy:

9.1 Making or forwarding defamatory remarks about any person or any organisation, including your colleagues.

9.2 Sending or forwarding discourteous electronic communications to colleagues or other third parties.

9.3 Sending electronic communications or attachments to electronic communications which are sexually or racially offensive or which breach the provisions or spirit of the Trust's Equal Opportunities Policy or Dignity at Work Policy.

9.4 Entering into contractual commitments on behalf of the Trust through electronic communications correspondence without the express consent and supervision of a senior manager.

9.5 Use of electronic communications facilities for the transmission of unauthorised private or personal electronic communications.

9.6 Sending, receiving or downloading through electronic communications any materials which may be copyright. You must consult a senior manager first if you are in doubt.

9.7 Disclosing through electronic communications any information about the Trust, its officers, employees, suppliers, users, or other business associates which you know to be confidential.

9.8 Mass communications or any other similar activity that could cause congestion, disruption of networks and systems, or interfere with the work of others.

9.9 The creation or forwarding of any electronic communications use involving chain letters or the distribution of junk mail.

9.10 E-mail should not be used to send large attachments which are not work related.

10 E-mail Account Limits

10.1 All Trust e-mail accounts are subject to set size limits depending on the license allocated. These are:

License	Size
F1	2GB
E5	50GB

10.2 All staff must observe and work within the limits set. Regular e-mail housekeeping will help staff to comply with these limits.

10.3 Any request for an increased limit must be submitted to your manager. The request will then be considered by the IM&T Directorate.

11 Monitoring of Electronic Communications

11.1 The Trust may monitor electronic communications at any time without prior notification when deemed necessary to do so. An employee may have access to any information which has been placed on their personal file following any monitoring of their electronic communications. Such monitoring would occur for reasons including, but not limited, to the following:

- Technical maintenance or problem resolution.
- Under subpoena, or a discovery request in a legal action.
- During an investigation into alleged misconduct, including unauthorised or excessive use of the e-mail system, or in connection with the prevention or detection of criminal or illegal actions.
- During an enquiry concerning compliance with this Policy.
- To establish the details of transactions or other matters relevant to the business of the Trust.
- To ensure compliance with regulatory or self-regulatory practices and procedures relevant to the business of the Trust.
- To ensure effective monitoring of the system including monitoring for viruses and other external threats, for old or obsolete files or for items which are absorbing a disproportionate amount of space on the system.
- For the purpose of determining whether or not a particular communication is relevant to the business for example during the absence of a member of staff on holiday or sick leave.

12 Authorisation to Use Electronic Communications

12.1 All managers are responsible for ensuring that staff have the access to those Trust systems and applications which they need to fulfil their role. This should be undertaken ready for induction.

12.2 An application to provide staff with access to electronic communications must be submitted to the IT Service Desk following standard procedures.

12.3 It is the manager's responsibility to inform the IM&T Service Desk of any post changes and of individuals who have left the organisation so that accounts can be amended or closed as appropriate.

12.4 IM&T maintain a record of all persons registered to use IT systems and a formal review of user accounts and access rights is conducted at regular intervals.

13 Use of NHS Mail and Directory Service (National Policy)

The use of NHS Mail is governed by the Department of Health, refer to their training and guidance at:

https://digital.nhs.uk/services/nhsmail

14 Relationship with Other Policies

This Policy will be supported by the following policies and procedures:

Disciplinary Policy

Electronic Information Security Policy

Electronic Communications Act 2000

Current data protection legislation

Appendix A: Equality Impact Assessment

<table>
<tr><th colspan="2">EIA Cover Sheet</th></tr>
<tr><td>Name of process/policy</td><td>Electronic Communications Policy</td></tr>
<tr><td>Is the process new or existing? If existing, state policy reference number</td><td>New</td></tr>
<tr><td>Person responsible for process/policy</td><td>IT Security & Resilience Manager</td></tr>
<tr><td>Directorate and department/section</td><td>IT</td></tr>
<tr><td>Name of assessment lead or EIA assessment team members</td><td>Chief Information Officer</td></tr>
<tr><td>Has consultation taken place?

Was consultation internal or external? (please state below):</td><td>No</td></tr>
<tr><td>Internal</td><td></td></tr>
<tr><td>The assessment is being made on:

Please tick whether the area being assessed is new or existing.</td><td>
<table>
<tr><td>Guidelines</td><td></td></tr>
<tr><td>Written policy involving staff and patients</td><td>X</td></tr>
<tr><td>Strategy</td><td></td></tr>
<tr><td>Changes in practice</td><td></td></tr>
<tr><td>Department changes</td><td></td></tr>
<tr><td>Project plan</td><td></td></tr>
<tr><td>Action plan</td><td></td></tr>
<tr><td colspan="2">Other (please state)

Training programme.</td></tr>
</table>
</td></tr>
</table>

Equality Analysis					
What is the aim of the policy/procedure/practice/event? **To set out the Trust's policy for the protection of the confidentiality, integrity and availability of the information it holds.**					
Who does the policy/procedure/practice/event impact on? None of the below					
Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐
Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐
Who is responsible for monitoring the policy/procedure/practice/event? **IM&T Security & Resilience Manager**					
What information is currently available on the impact of this policy/procedure/practice/event? **None**					
Do you need more guidance before you can make an assessment about this policy/procedure/ practice/event? **No**					
Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? Yes/No, If yes please provide evidence/examples:					

Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐
Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐

Please provide evidence:

This policy does not have any impact on any protected characteristics

Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics? Yes/No, if so please provide evidence/examples:

Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐
Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐

Please provide evidence:

This policy does not have any impact on any protected characteristics

Action Plan/Plans - SMART

Specific

Measurable

Achievable

Relevant

Time Limited

Evaluation Monitoring Plan/how will this be monitored?

Who **IM&T Security & Resilience Manager**

How **Via feedback**

Reported to **Chief Information Officer**

Appendix B: Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Malicious: content sender attachments	Trust IT and Microsoft	IT technical defences, internal and Office365	Constant	Dashboard and email alerts	Report ti IM&T accountability group	IT	Discuss by management and disseminated to the appropriate staff