South Eastern Health and Social Care Trust

Policy Code: SET/Gen (12) 2018

SOUTH EASTERN TRUST

Title:	**ICT - Email Management Policy**			
Author(s)	**Assistant Director of Technology & Telecommunications**			
Ownership:	**South Eastern Health & Social Care Trust**			
Approval by:	**Ratified Directors as per signatory list**		**Approval date:**	**September 2016**
Operational Date:	**April 2018**		**Next Review:**	**March 2023**
Version No.	**2.1**	**Supercedes**	**SET/Gen (12) 2018 V2.0**	
Key word/s	**Email**			
Links to other policies	**ICT – Master Policy** **ICT - Security Policy** **Email encryption guidance**			

This policy should be read in conjunction with the Trust ICT Security Policy

1.0 INTRODUCTION

1.1 Background

1.1.1 Increasingly e-mail is being seen as the preferred mechanism for communicating internally within the Trust and externally to other organisations. Whilst acknowledging the advantages to all parties in using this technology, staff must accept the need to be professional in approach whenever communicating, irrespective of the medium. Moreover email has increased accessibility for staff as well as service users.

1.1.2 Unlike other forms of communication there are some security issues with e-mail including the inadvertent introduction of computer viruses and the danger of messages being read by individuals who are not the intended recipient. This is particularly so for e-mails which are sent to, or received from any accounts which are external to the HSC network.

1.1.3 This policy applies to any electronic mail whether internal, issued to, or received from external sources to the HSC network.

1.1.4 Email is a record of business activities and transactions and need to be managed effectively like any other record.

1.1.5 All emails within the Trust form part of the public record and are subject to disclosure in the event of PSNI investigation or under legislation such as Freedom of Information.

1.1.6 Staff should be aware that emails are corporate assets and email accounts may be subject to Trust scrutiny under authorisation of the relevant Assistant Director.

1.2 Purpose

1.2.1 This policy provides a summary of the required principles, values, structures and roles and responsibilities of all staff to support the on-going implementation and application of ICT to positively inform Trust core objectives.

1.2.2 This policy should be read in conjunction with other related Trust ICT Policies.

2.0 DEFINITIONS/SCOPE OF THE POLICY

2.1 This policy sets out the obligations that all Trust employees have when dealing with email messages. The following practices outlined in this policy will ensure that the Trust meets its legislative, operational, and accountability requirements.

2.2 This policy applies to all staff that use Trust email resources.

3.0 ROLES/RESPONSIBILITIES

3.1 The Assistant Director of Technology and Telecommunications is responsible for this policy. The ICT Services Manager will provide appropriate technical and staff resources to support policy implementation and adherence. Line managers are responsible for implementation and ensuring adherence to this policy.

3.2 All members of staff are responsible for identifying and managing email messages that constitute a record of their work.

4.0 KEY POLICY PRINCIPLES

4.1 Key Policy Statement

The Trust employs email as a business communication tool to enable Trust staff to communicate both effectively and safely within and external to the Trust.

4.2 Is an Email Message a Record?

4.2.1 A **Record** is recorded information in any form that is created or received by the Trust in the transaction of its business or in the conduct of its affairs and which it retains as evidence of such activity.

4.2.2 The types of emails to be retained include:

4.2.2.1 messages that reflect the position or business of the Trust;
4.2.2.2 messages that initiate, authorise, or complete a business transaction;
4.2.2.3 messages received from external sources that are clearly of interest to the Trust in the conduct of its business;
4.2.2.4 drafts that show the evolution of a document as it goes through the approval processes;
4.2.2.5 original messages of policies or directives;
4.2.2.6 Agenda and minutes of meetings; briefing notes.

4.2.3 The types of emails which should be deleted include:

4.2.3.1 messages that are duplicate copies of information;
4.2.3.2 duplicate copies used for information or reference purposes only;
4.2.3.3 messages of additional information which has been incorporated into subsequent versions;
4.2.3.4 rough or working drafts that are not required to document the steps in the evolution of a document;
4.2.3.5 miscellaneous notices of employee meetings, holidays, etc.;
4.2.3.6 messages received as part of a distribution list or received from other Internet sources solely for convenience or reference;
4.2.3.7 Junk mail or any other unsolicited material such as mass mailings (e.g. Christmas (PowerPoint) greetings), advertisements, jokes, images or chain letters. (These should be deleted immediately as they waste staff time, slow access and in some cases may lead to a breach of IT Security Policy).

4.3 Why Do We Need to Manage Email?

The Freedom of Information Act (2000) requires the Trust to respond to all requests for information from anyone in the world in respect of any recorded information that it holds and in any form; and this includes email.

4.4 Guidance on the use of email

4.4.1 The email system must not be used to transmit patient/client identifiable or confidential information to any recipient outside the HSC network unless approved.

4.4.2 Encryption must be applied to any content that is deemed sensitive or contains patient/client information sent to a non hscni.net email address where approval has been given as per 4.4.1

4.4.3 Examples of sensitive and personal information include but are not limited to:-

4.4.3.1 copies or extracts of data from clinical systems;
4.4.3.2 commercially sensitive information;
4.4.3.3 contracts under consideration;

4.4.3.4 budgets;
4.4.3.5 staff reports;
4.4.3.6 appointments – actual or potential not yet announced;
4.4.3.7 disciplinary or criminal investigations.

Please refer to SETrust HSCNI email encryption guide published on i-connect.

4.4.4 Personal use of Trust email should be restricted so that it does not interfere with work commitments

4.4.5 Personal Trust email addresses **must not** be used for registration or subscription to internet sites e.g. Tesco, Amazon, Groupon

4.4.6 Staff should restrict the recipients of e-mail messages to those who actually may have interest in the message contents. Staff should consider use of i-connect as an alternative method for posting such general information. This can be accessed through the ICT service desk.

4.4.7 The use of "all users" emails is restricted. In the event of persons wishing to use this facility they should contact the ICT service desk.

4.4.8 The email system must not be used to transmit inappropriate, obscene, offensive, damaging, defamatory, threatening material or material intended to frighten or harass. If staff are in receipt of such an email they should seek advice from their respective Line Manager.

4.4.9 Users must not generate and/or forward an email which is offensive to any individual or group, based on race, religion, ethnicity, political opinion, age, gender, marital status, sexual orientation or disability. This includes jokes, advertisements and chain letters. Any material which is discriminatory, or encourages discrimination, may be unlawful under Equality and Human Rights legislation. Staff in receipt of such an email should seek advice from their respective Line Manager.

4.4.10 The email system must not be used to infringe copyright.

4.4.11 Any suspected Spam or Phishing email should be reported via the "report spam" button on outlook.

4.4.12 The email systems should not be used to attempt unauthorised access to other networks or systems.

4.4.13 The email systems should not be used to conduct unsolicited advertising or similar activities.

4.4.14 Staff should check e-mail inboxes regularly and provide responses relative to the importance of the message. If appropriate, staff planning leave should consider re-routing e-mail or providing shared access to a trusted colleague in the same way that they might make arrangements for postal mail to be opened and processed in their

absence. Staff should use out of office messaging or mail diversion functionality when appropriate.

4.4.15 Staff will be held accountable for all e-mail originating from their own account therefore password protection is of utmost importance. Single sign on should be used to enable multiple users to efficiently access a single ICT point concurrently.

4.4.16 Email messages must be clear and concise and the tone and content must be suitable for a business communication and appropriate to the medium.

4.4.17 Attachments can be sent but a limit on file size applies. Contact ICT service desk as appropriate.

4.4.18 Emails deleted from email account will be recoverable for a minimum of 2 weeks after their deletion.

4.4.19 Unauthorised access to other users' e-mail accounts is prohibited.

4.4.20 In the event of the ICT Department receiving a request for access to an absent staff members email account by another staff member in order to retrieve work related correspondence the ICT Department will follow the following authorisation protocol:

The staff member requesting access to the absent staff members email account ('Owner') will need to supply the ICT Department with written notification/authorisation from the Owner or in the event of that staff member being unavailable from the associated Assistant Director.

5.0 IMPLEMENTATION OF POLICY

5.1 Dissemination

5.1.1 This policy will be brought to the attention of all Line Managers within the Trust who will ensure that all staff that utilise ICT are fully aware of the provisions of this policy.

5.1.2 This policy will be posted on the Trust Intranet site.

5.2 Resources

As part of the Trust Induction Programme, all new staff will be sign posted to where they can receive a hard/soft copy of Trust policies.

5.3 Exceptions

Nil

6.0 MONITORING

The Trust will monitor and manage compliance to this policy utilising appropriate software systems and associated practice to filter and delete inappropriate, obscene, offensive or damaging material received via the Trust Email System for the purposes of reducing the risk associated with Computer Viruses or Email SPAM.

Failure to comply with this policy may result in disciplinary action.

7.0 EVIDENCE BASE / REFERENCES

Professional Records Standard Body (PRSB) - Guidelines for using email in health and social care

8.0 CONSULTATION PROCESS

This policy was circulated to Trust's policy consultees for consultation and comment

9.0 APPENDICES / ATTACHMENTS

Not Applicable

10.0 EQUALITY STATEMENT

In line with duties under the equality legislation (Section 75 of the Northern Ireland Act 1998), Targeting Social Need Initiative, Disability discrimination and the Human Rights Act 1998, an initial screening exercise to ascertain if this policy should be subject to a full impact assessment has been carried out.
The outcome of the Equality screening for this policy is:

Major impact ☐

Minor impact ☐

No impact. x

SIGNATORIES

(Policy – Guidance should be signed off by the author of the policy and the identified responsible director).

Policy Name	Author Endorsement	Modified	Modified By
Email Management	Yes	30/03/2017 11:55 AM	Stewart, Stephen

Policy Name	Approval	Modified	Modified By
Email Management	Endorsed	19/04/2017 02:18 PM	Coulter, Roisin
Email Management	Endorsed	09/03/2018 03:33 PM	McCaughey, Hugh