Western Health and Social Care Trust

ELECTRONIC MAIL (E-MAIL) POLICY

October 2017

Version 4.1

Policy Title	ELECTRONIC MAIL (E-MAIL) POLICY
Policy Reference Number	CORP09/006
Implementation Date	WITH IMMEDIATE EFFECT FOLLOWING APPROVAL BY TRUST BOARD
Revised Date	October 2017
Approved Date	ICT SMT Approval – 6/11/17 PSI SMT Approval – 27/11/17 Trust CMT – 14/12/17 Trust Consultation Approval – 17/01/2018 Trust Board Approval – 01/02//2018
Review Date	February 2020
Responsible Officer	FERGAL DUREY, AD for ICT and Telecommunications

Table of Contents

1. Background and Purpose

Electronic mail (E-mail) is a significant business, information and communication tool for the Western Health and Social Care Trust (WHSCT) and staff need to be aware of their personal responsibilities with regards to its use and the potential consequences resulting from misuse.

Any correspondence sent or received via the Trust e-mail system is considered as a public record and will fall under the requirements of the Freedom of Information (FOI) Act 2000 (corporate/business related information) or the Data Protection Act 1998 (personal information).

The measures outlined in this policy will not be effective without the cooperation of all Western Trust staff. These include full-time, part-time, 3rd party consultants contracted by the Trust to work on specific projects, agency and temporary employees. The cooperation of all such staff, and acceptance of this policy, is therefore a prerequisite to approval for e-mail access.

The purpose of this policy is to ensure proper and appropriate use of WHSCT's corporate e-mail and associated communications technologies systems by making staff aware of the organisation's definition on acceptable and unacceptable use.

E-mail is a communication tool and <u>not</u> a replacement for any Trust information system.

Communications via e-mail about a patient, client or staff member may also be deemed to be part of that individual's personal record, in the same way as a letter would, and departments should consider whether this should be printed and included in the patient/client/staff file.

Failure to comply with this policy may lead to disciplinary action.

2. Cybersecurity

Trust staff need to be aware of the risks and potential for loss of data, equipment or embezzlement of funds via Cyberattacks.

*A **cyberattack** is any type of offensive manoeuvre employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys systems or attempts to embezzle users/businesses.*

Cyberattacks can take multiple forms and the following are a few examples;

- Hacking – someone gaining unlawful access to the ICT network, computer, laptop etc and potentially deleting files and/or stealing data.
- Malware – malicious software that can do any number of things e.g. delete files, make systems crash or target communications equipment.
- Ransomware – where a piece of malicious software runs on a PC, laptop or server, and encrypts (garbles) all the data on the device and therefore makes it no longer usable. There is no guarantee that if the guarantee is paid that the device will decrypt or that encryption will reoccur!

"Wannacry" was an example of a worldwide ransomware (cyber) attack in May 2017

3. Risks associated with the use of E-mail

- Opening an e-mail which introduces a piece of malware/ransomware to the PC or Trust network
- Responding to any e-mail which requests user account/password or personal details
- Information could be sent to the wrong person with the same or similar name
- E-mails can be read by someone other than the intended recipient
- Possible loss of information or inappropriate access if the e-mail system is compromised
- Data loss due to sending information to insecure networks
- Confidential information sent in open e-mail may be less secure than information sent by post in a sealed envelope.
- Breach of the Data Protection Act (DPA) if information contained within an e-mail is not deleted and is therefore retained by the Trust for longer than is necessary.
- Confidential information sent by e-mail will be retained within the e-mail system even if deleted from personal computers.
- Inappropriate language or content being used

4. Obtaining an E-mail Account

Access to Trust e-mail services will be provided upon receipt of a properly completed "Request for New User Account" form (available on the Trust Intranet under ICT).

Managers should note that there may be a cost associated with the creation of an e-mail account.

The set-up and management of all user accounts is governed in accordance with guidelines and principles found in the *WHSCT Management of User Accounts and Password Policy*.

5. Guidelines for users

E-mail traffic **within** Health and Social Care (HSC) networks(i.e. e-mail addresses ending in one of the following) may be regarded as secure and protected;

'.hscni.net'
'.n-i.nhs.uk'
'.ni.gov.uk'
'.ni.gov.net'

however the risk that e-mails can be read by someone other than the intended recipient is real and cannot be ignored. This is particularly the case when e-mail is sent or received via less secure networks such as Internet web mail.

The use of e-mail to transmit patient or client identifiable information raises particular issues and concerns for the Trust, particularly with respect to the following legislation:

- The Data Protection Act (DPA) places an onus on organisations handling personal data to employ and promote standards that will ensure the patient's / client's right to privacy – and places a separate obligation on any member of staff or individual processing or handling information of a personal nature to maintain the confidential nature of that information.
  The 7th principle of the DPA states that *"appropriate technical and organisational measures shall be taken against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".*
- The Freedom of Information (FOI) Act 2000 provides the general public with rights of access to the information held by public authorities.

Personal-identifiable information sent by e-mail within the Western Trust or to Trusts and other agencies *within* the HSC must be done within the requirements of the Data Protection Act. Individual staff members are responsible for ensuring the confidentiality of information they send by e-mail.

Information can be transferred across the HSC e-mail network in the knowledge that the system is secure and protected; however staff should still protect any file attachments that are sensitive or contain personal/patient level information.

In cases where electronic transmission of this type of information is unavoidable, staff should consider whether to encrypt the content of an e-mail particularly if sending

patient identifiable information externally (outside HSC network). Appropriate encryption must be used as mandated in the DHSSPNI approved standard. Communication to the Criminal Justice System should follow the approved procedure. For more information on how to encrypt e-mails please refer to the appendices.

Taking both confidentiality and patient safety into account, steps should be taken where possible to anonymise the information being sent by e-mail.

Where necessary, a delivery receipt should be requested with e-mail containing sensitive / personal data

Personal-identifiable information must *not* be sent by e-mail outside the HSC network unless proper security measures are in place, including encryption and pass-word protection of data.

In all cases, only the minimum information must be sent by e-mail and great care must be taken to ensure the correct e-mail address is used.

Personal information about service users or staff should not be e-mailed either to or from any staff member's personal computer or personal e-mail account.

***Staff must never* e-mail Trust user account and/or password details.**

Before sending any confidential information by e-mail, staff should consider the following: -

- Does the e-mail need to be sent?
- Do all intended recipients really need to see it?
- Do I really need to include attachments containing confidential details?
- How urgent is it? Is there another more secure way of sharing the information?
- In the case of patient/client information, is it already available to the intended recipient on one of the Trust patient administration systems?

The Trust **does** employ Countermeasures and Endpoint security (refer to Section 8) which is protecting the Trust from known or potential security problems however, when there is a brand new virus, or type of malware, there may be no countermeasures available for some days.
Staff are always advised to;

- ensure that their PC, laptop etc is connected to the Trust network so that the latest countermeasures and security patches can be applied.

- exercise caution when a web site, or e-mail, directs the user to another web page link.

- ensure that the web link is spelt correctly as many unscrupulous web sites use modified legitimate addresses e.g. www.rightaddress.co.uk is correct but the following has a changed character www.rlghtaddress.co.uk

- **not** respond to **any** e-mail, or web site, that requests you to change your password **or** to provide personal details. “If in doubt – check it out” directly with Trust ICT, 3rd party provider etc.

- pay attention to the style, context, wording and spelling used on the web site but particularly within emails. Many fraudsters will use legimate company logos and screen layouts to convince and persuade the user of their authenticity. This technique is referred to as “social engineering”.

- **think** - is there something about the web page, or e-mail, that does not look right or is a little off? Too good to be true? Trust your instincts if they tell you to be suspicious. **If** in doubt, close the e-mail or web page.

For advice and guidance on Records Management including a retention and disposal schedule refer to the following website; www.dhsspsni.gov.uk/topics/good-management-good-records. The reader should note that the retention of e-mails is determined on the content within an e-mail.

Personal Use

- Staff are not restricted from using Trust e-mail for their own personal use but this must be within their own time and must not interfere with other staff carrying out their work duties
- Staff **must** not register their hscni.net mailbox with **retail** websites for personal use e.g. Amazon, Groupon. Private e-mail accounts should be used in these cases as use of hscni.net mailboxes could potentially increase the amount of spam sent to the HSC. Where a member of staff has already registered their work e-mail account they should take steps to remove this immediately.
- Staff should permanently delete personal e-mails as soon as possible. This includes the Inbox, Sent Items and Deleted Items. Where staff need to **retain** personal e-mail, it is advised that these should be moved to a specific folder labelled Personal and/or clearly marking them in the subject line as Personal.
- Personal information about patients, clients or staff should not be e-mailed either to or from staff member’s personal e-mail accounts.
- Staff are not to auto-forward or send any e-mail from their Trust e-mail account to personal e-mail accounts **or** from personal e-mail accounts to Trust e-mail accounts.
- The user must not create any unauthorised contractual liability on the part of the Trust.
- Unauthorised access to staff e-mails and messaging, business or private, is strictly prohibited.
- The Trust will not accept any liability for financial loss while using Trust systems for personal transactions.
- The Trust reserves the right to monitor the e-mail system.
- Users might be personally liable to prosecution, and open to claims for damages, if their actions are found to be in breach of the law

Tone and Content

- Business related e-mails should be concise yet formal.

- E-mails with content that may be deemed offensive (including e-mail attachments) should not be sent or forwarded. This may lead to disciplinary action.
- Staff should refrain from sending e-mail that:-
    - May potentially infringe copyright
    - Contains defamatory or threatening comments
    - Requires the recipient to forward to further recipients for no business purpose (i.e. chain letters)
- Staff should note that the above also applies to the Microsoft Lync application. This application can also generate e-mail.
- For further guidance on Good Practices and Email Etiquette refer to Appendix 2

All business related e-mails are potentially discoverable documents under the terms of the Freedom of Information (FOI) Act or associated legislation.

6. Encryption

Encryption is the process of encoding messages or information in such a way that only authorised parties can read it.
Staff should be aware that there **is** a different process to follow when encrypting information for sending by e-mail within the HSC network and sending to external organisations (outside HSC network). Staff are advised to refer to Appendix 6 below for further guidance.

7. Incident Reporting

Staff should report any actual or suspected breaches of confidentiality or data security in the secure operation of the Trust e-mail system via the Trust's Incident Reporting Policy and Procedures.

8. Countermeasures

This policy should be seen as one of a number of countermeasures put in place to protect the organisation and its employees from such things as inadvertent exposure to illicit material, malicious software etc, and also the possibility of legal action that may result directly from e-mail abuse or misuse. Additional protection is provided by the following:-

- **Endpoint Security**
  All computers have Endpoint (*anti-Virus* software) installed. The software runs continuously and is updated with the latest version several times a day. Microsoft security patches are applied, on a regular basis, to all PC's, servers and laptops that are connected to the Trust network.
  Users of other third party devices/modalities that are attached to the Trust network must make special arrangements to have Endpoint software installed via the ICT Service Desk.
  As part of the Endpoint control measures, certain e-mail attachments are blocked from entering or exiting the HSC network. If an attachment is blocked the user is informed via e-mail of the steps to take to request its release.
- **Content Filtering**
  All e-mail content (including attachments) is filtered. Content filtering is used to aid the detection and removal of spam e-mail. Filters are refined on a daily basis;

however users may still find these types of messages in their Inbox. Upon discovery users should forward these items to **spam@westerntrust.hscni.net**

- **E-mail Archiving**
  All e-mail (sent or received) is electronically archived to assist in the Trust's compliance with certain legislation (e.g. Data Protection Act 1998 and Freedom of Information Act 2000)
- **Monitoring**
  i) The Trust reserves the right to monitor the e-mail service and may, with appropriate approval, open messages in the absence of a member of staff.
  ii) Suspected cases of abuse on the system or breaches in policy will be rigorously investigated by ICT, and where necessary, in conjunction with HR staff.
- **Removal**
  i) Access to the e-mail services may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected abuse or misuse
  ii) E-mail accounts will be terminated (and e-mail archived) for staff who leave the organisation
  iii) Dormant e-mail accounts, or accounts not otherwise accessed on a regular basis (6 months), will be deemed suitable for suspension. Special leave or periods of extended absence will be taken into consideration.

9. Additional Resources

This policy should be read in conjunction with other policies relating to effective and appropriate use of ICT services, including

1) WHSCT Internet Policy
2) WHSCT Management of User Accounts and Password Policy.
3) WHSCT Server, Desktop and Portable Security Policy
4) WHSCT Malicious Software Policy
5) WHSCT Disposals Policy (including redistribution of ICT equipment)
6) Good Management Good Records DHSSPS
7) WHSCT Data Protection & Confidentiality Policy
8) WHSCT Incident Reporting Policy and Procedures
9) *Freedom Of Information & E-mails Guidance* DHSSPS – Code of Practice on Protecting the Confidentiality of Service User Information
10) Information Commissioner – Anonymisation: managing data protection risk – code of practice (www.ico.gov.uk)
11) Information Commissioner – Data sharing code of practice (www.ico.gov.uk)
12) Regulation of Investigatory Powers Act 2000
13) BSO ICT policies

10. Training

The Trust is committed to staff development and seeks to consistently improve development standards and opportunities for staff in line with organisational objectives, policies and procedures. Should you or your staff require support in the effective use of ICT please contact the ICT Training Team via the ICT Service Desk.

11. Equality & Human Right's Statement

The Western Health & Social Care Trust's Equality and Human Right's statutory obligations have been considered during the development of this policy.

12. Further Information

For further information in relation to this policy please refer to:-

The ICT User Forum on the ICT service desk portal available on the Trust intranet link below.

(http://wta-eservicedesk/portal/)

Appendices

Appendix 1: General Advice

1. Ensure you send your e-mail and any attachments **only to people who need to see it**. Identify the correct person to receive your e-mail. Only copy those who really need to see the e-mail

2. Always be sure that you have the correct recipient before sending the e-mail. Take extra care when there is more than one person on the e-mail system with the same or similar name.

3. You should include a standard signature at the bottom of your e-mails including: your name, job title, organisation name and contact details. Do not use graphics, animation or images of your signature.

4. Only mark e-mails as important if they really are important

5. Always use the subject box, in line with records management arrangements , providing a short description of the subject and its urgency.

6. Do not include personal details on e-mail Subject line

7. Do not open, or respond to, e-mail requests from unknown or external sources which request personal or sensitive information (known as Phishing).

8. Do not open, or repond to, e-mails, especially those with any attachments, from unknown or dubious sources.

9. Do not send unnecessary attachments,

10. Do not print e-mails unless you really need to for work purposes.

11. Do not leave your e-mail open and unattended – use a password protected screensaver

12. Delete any e-mail messages that you do not need to have a copy of.

13. Do not use the deleted items folder for storing required or important e-mails. It is considered good practice to “empty” the deleted items folder either on a daily basis or when you exit the e-mail system. E-mails within this folder will be purged on an ongoing basis by ICT.

14. Out of Office should be enabled, with an appropriate message,if staff are out of the office or unable to respond to e-mail for extended periods.

15. Update your details on the Trust E-mail system (outlook properties) and encourage others to do so. This will help staff to identify the right person before an e-mail is sent and reduce the risk of information being sent to the wrong person.

16. Unauthorised access to other users’ e-mail accounts is prohibited

17. Be careful of **any** e-mail that places time limits i.e. “if you don’t respond within 48 hours your account will be closed” or “a response is needed within the next ….”. Confirm the source **and** the requirement before responding.

18. Before responding to an e-mail, check the e-mail address provided, as fraudsters may slightly altered it e.g. mary.oneill@anytrust.hscni.net is correct but mary.oneill@anytrust.hsoni.net is incorrect.

19. Be suspicious of any e-mail, including HSC, which requests the user to respond to an alternative e-mail address.

20. Staff are reminded that where there has been a serious loss of personal data it should be brought to the Information Commissioner. If the Trust is found liable then the Commissioner can apply a stiff financial penalty. If data on a PC, laptop etc becomes corrupted then there is the risk of data loss if the data has not been regularly backed up. When a device has been encrypted there will be a significant delay to the user and/or service until the device has been fully restored.

21. Staff are advised to contact the ICT Service desk where they have doubts regarding the content or origin of suspicious e-mails.

Appendix 2: Good Practices and Email Etiquette

- **Consider content & wording carefully**, and do not use e-mail to start an emotive or sensitive exchange. If a topic is likely to require discussion, a conversation or meeting may be more appropriate and professional. Keep the content brief and concise. In some cases it may be necessary to tailor the message to the recipients cultural background. Remember that once you send an email, it's virtually impossible to get it back!
- **Be Polite & Professional** – laws, protocols, codes of conduct and rules of etiquette apply to e-mails as much as paper based correspondence. For example, the use of CAPITALS or **Bold Type,** emoticons, emojis and slang are to be avoided as are the use of sarcasm and humour in any content.
- **Help Your Recipients** - Use Effective Subject Titles to easily let the recipients know what you expect from them e.g. **ACTION, INFORMATION, REVIEW**
- **Signature** – Not everyone knows who you are! Therefore, end your email with some information about you e.g. full name, job title, Western Health & Social Care Trust and contact details
- **Protect It** – Remember that information security practices apply to e-mail. Ensure you have permission to forward a restricted or sensitive e-mail, and take appropriate steps to secure sensitive data e.g. using encryption.
- **Attachments** – Add these to the email *first,* before composing the email body. That way you can not forget to attach them! Ensure any attachment containing person identifiable data is encrypted.
- ***Think* before sending** –
  I. Review the recipient list and addresses for accuracy and consider whether the receipient really needs the mail.
  II. Ensure no person identifiable data appears in the Subject line.
  III. Does the email of its content need encrypted?
  IV. *Proof read* the email body. Do not rely on the spell checker.

E-Mail Housekeeping Principles

1. Regularly review your mailbox
2. Decide whether an e-mail message has to be "deleted" or "retained"
3. Detach & file "retained" e-mails to an appropriate record storage location
4. Delete unwanted or unneeded e-mails
5. Don't forget to clear out Deleted Items and Sent Items folders

Examples of **"deleted"** could be:	Examples of "**retained"** could be:
• Personal e-mails • Meeting acceptance e-mails • "For Information" E-mails • Bulletin messages • Low priority messages • Routine, low level activities • Duplicate copies of meeting papers • Duplicate copies of reports • "Read" or "Delivery" receipts • Trust and Network Admin E-mails	• Relating to business decisions • Relating to Management of Staff or Contracts • Evidence that something was acted upon or took place • Evidence of significant elements of your work including projects

Appendix 3: Safe E-mail Transmission Procedures *for Confidential or Sensitive information*

In cases where transmission of this type of information by e-mail is unavoidable, when creating or sending an e-mail, staff should:

1. Avoid sending excessive amounts of confidential information by e-mail. Only send the minimum amount of information required
2. Only send information to those who need to receive that information for a specific purpose.
3. Do not copy (cc) or 'forward' the e-mail unnecessarily to other staff.
4. Ensure the e-mail goes to the correct person.
    a. If you are not sure if you have the right person or the right e-mail address, you must check this before sending any information.
    b. Where there is more than one person with the same name or with similar names on the e-mail list, please make sure you have selected the right person. If you are unsure check before sending.
    c. If sending regular e-mails to a certain person, save them into your 'contacts' and chose the name from there rather than the general e-mail list.
    d. Request that the recipient e-mail his/her request for information and then send information using the 'Reply' button.
    e. When using the 'reply to all' button, be careful only to send information to appropriate person(s).
5. Do Not include names, addresses or other identifiable information in the subject line of an e-mail.
6. Do Not type confidential information, especially sensitive personal information, into an open e-mail. Type into a separate document (e.g. MSWord document) and send as a secure attachment.
7. All reports that include sensitive personal information should be **pass-worded** and **encrypted** to provide an extra level of protection. The pass-word should only be disclosed to the intended recipient (e.g. by phone or in a separate e-mail). Seek advice from ICT department on how to encrypt a document.
8. Ensure appropriate level of encryption is used (see links) . Note:- there **is** a difference between encrypting information for sending internally within the HSCand for external distribution (outside the HSC network). Staff are advised to refer to the Trust Encryption Policy and the Appendices below for further guidance. Consider sending anonymised information (removing identiafiable data) or pseudonymised information (sending personal Identifiers such as name, address etc. separate from other information e.g. linked by a unique code)
9. To ensure the confidentiality of sensitive personal information (e.g. reports regularly sent internally within a staff group) other means of communication should also be considered, for example, by post and suitably marked.
10. Confidential information received by e-mail should be printed and/or saved in the relevant file and deleted from the Trust e-mail system.

Appendix 4: Receiving confidential information by e-mail

1. If personal or confidential information is received in error via e-mail by a member of staff, the sender should be contacted immediately and advised of this and agree further action required.

2. Personal or confidential information received in error by e-mail should not be forwarded by return e-mail or to other staff via e-mail. The sender should be contacted to advise of the data breach and arrangements made to delete the information from the recipient's inbox and deleted mail folder.

3. In circumstances where personal or confidential information is received from an unidentified sender, this should be brought to a manager's attention.

4. Staff should report to their line manager situations where personal or confidential information is received inappropriately on more than one occasion from the same sender.

Appendix 5: E-mailing Sensitive Information to a new contact

It is recommended that the following simple mechanism is employed when transmitting information to a new contact or to an officer you have not e-mailed previously.

Step 1. Contact the recipient and ask for their e-mail address.

Step 2. Send a test e-mail to the address provided to ensure that you have inserted the correct e-mail address.

Step 3. Ask the recipient on receiving the test e-mail to reply confirming receipt.

Step 4. Attach the information to be sent with a subject line 'Private and Confidential, Addressee Only' to the confirmation receipt e-mail and send.

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

I. copies or extracts of data from clinical systems;
II. commercially sensitive information;
III. contracts under consideration;
IV. budgets;
V. staff reports;
VI. appointments – actual or potential not yet announced;
VII. disciplinary or criminal investigations.

Appendix 6: Encrypting an E-mail or E-mail file attachments

Staff are referred to the WHSCT ICT User Sharepoint site for up to date instructions on how to encrypt an e-mail or an e-mail attachment.

Staff should note that there are different encryption processes to follow, depending on whether the e-mail is to be sent internal within the HSC network or to an external organisation

To access these instructions, enter the following link on a Web Browser;

http://sharepoint.westhealth.n-i.nhs.uk/sites/it/users/SitePages/ictfaqsMain.aspx

When the ICT User Site web page appears, select the General tab

Encryption procedures described are;

1. Encrypted Mail Procedure (Emailing outside of Western Trust)

   This procedure describes how to encrypt an e-mail message which is to be sent to an external e-mail address.

2. J-Zip – How to encrypt documents for email (E-mailing inside the HSC network)
   Encrypt Documents using PeaZip

   These procedures describe how to encrypt e-mail attachments.
   Either program can be used. The dependency is on which version of software is installed on the PC or laptop.