Western Health and Social Care Trust

ELECTRONIC MAIL (E-MAIL)

September 2014

Version 3.1

Policy Title	ELECTRONIC MAIL (E-MAIL) POLICY
Policy Reference Number	CORP09/006
Original Implementation Date	September 2009
Revised Date	September 2014
Approved Date	November 2014
Review Date	November 2016
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.

Email is a communication tool and <u>not</u> a replacement to any Trust information system.

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

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.

The measures outlined in this policy will not be effective without the cooperation of all Western Trust staff. The cooperation of all such staff, and acceptance of this policy, is therefore a prerequisite to approval for e-mail access.

2. 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 email 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*.

3. Guidelines for staff

E-mail traffic within Health and Social Care (HSC) networks may be regarded as secure; 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 Trust employs a range of patient / client administration systems to manage healthcare data and, in accordance with DPA principles, access to these systems is granted to all professionals, clinicians and admin support staff whose work necessitates it. In the main this should remove the need to send patient / client data via e-mail to individuals or agencies operating within or outside the HSC network.

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 Freedom of Information (FOI) Act 2000 provides patients and clients with rights of access to the information held by public authorities.

However, in cases where transmission of this type of information is unavoidable, staff should ensure:

I. Approval has been received and a *Data Access Agreement* must be in place.
II. Appropriate encryption must be used as mandated in the DHSSPNI approved standard. For more information on how to encrypt e-mails please refer to the procedure listed on the Intranet Website (under ICT, E-mail encryption).

Further material on the use of e-mail can be found on the Intranet site. Refer to Guidelines, procedures and protocols section and document titled "Protocol for the Electronic Transmission of Confidential Information".

***Never* e-mail Trust user account and/or password details.**

Personal Use

- Must be within staff's own time and not interfere with other staff carrying out their work duties
- 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 service.
- 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. These may lead to disciplinary action.
- Staff should refrain from sending e-mail that:-
  I. May potentially infringe copyright
  II. Contains defamatory comments
  III. Requires the recipient to forward to further recipients for no business purpose (i.e. chain letters)

All e-mails are <u>discoverable</u> documents under the terms of the Freedom of Information (FOI) Act.

External Webmail on Trust Devices (E-mail on the Internet)

- Only access to *doctors.net.uk and approved web mail services* will be allowed via a web browser
  Further exceptions will be at the discretion of the AD for ICT and Telecommunications.

4. 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.
  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 and Freedom of Information)
- **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 within HR guidelines and 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.

5. 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 Protocol for the Electronic Transmission of Confidential Information by Fax and Email
6) WHSCT Social Media Policy
7) *Freedom Of Information & E-mails Guidance (issued by WHSCT Communications Department)*

8) DHSSPS – Code of Practice on Protecting the Confidentiality of Service User Information
9) Information Commissioner – Anonymisation: managing data protection risk – code of practice (www.ico.gov.uk)
10) Information Commissioner – Data sharing code of practice (www.ico.gov.uk)
11) Regulation of Investigatory Powers Act 2000
12) BSO ICT policies

6. 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.

7. 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.

8. 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/)