THE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST

PERSONNEL POLICIES & PROCEDURES

EMAIL AND ELECTRONIC COMMUNICATIONS POLICY

Effective from: March 2007 **Review Date:** March 2010

1 Introduction.

1.1 This policy statement provides specific instructions on the use of electronic mail (e-mail) and other electronic forms of communication resident on personal computers and servers within the Newcastle upon Tyne Hospitals NHS Foundation Trust.

1.2 The use of email, and other forms of electronic messaging, is recognised as an essential tool to support the administration and communication of patient information. However the ease of transmission of clinical information must be constrained by adequate security protocols and guidance.

1.3 The Caldicott Guidelines were drafted to support the implementation of the Data Protection Act 1998 in the NHS. The Data Protection Act 1998 classifies clinical information as 'sensitive' information. This classification places additional requirements on organisations and individuals with regard to ensuring the secure processing of clinical information.

1.4 The Caldicott Guidelines and NHS policy require that ALL patient related information is processed only using secure NHS email accounts. Commercial and academic email and messaging services are not considered to be secure. These do not meet the standards required by the NHS or Data Protection Act 1998.

1.5 In order to ensure patient safety ALL clinical staff are required to regularly review the messages in their NHS email accounts, at least on a weekly basis or more frequently if required, to ensure that correspondence and messages relating to patients are acted on promptly.

In the relation to periods of leave or absence 'Out of Office' messages should be used were necessary to inform correspondents of alternate contacts for the relevant period.

1.6 Individuals who knowingly transfer confidential identifiable patient information to unsecured services are at risk of breaching the Data Protection Act 1998 and may be subject to any penalties that could be imposed. Commercial or academic messaging service suppliers will not indemnify users for breaches of the Data Protection Act 1998 arising from their actions.

1 Scope of Policy.

1.1 The policies apply to Newcastle upon Tyne Hospitals NHS Foundation Trust (The Trust) to all people who use or work the Trust, including employees, honorary contract holders, researchers, trainees, clinical observers and other contractors or individuals involved in patient care and covers e-mail and messaging `systems used through Trust computers and servers if these systems are under the jurisdiction and/or ownership of the Trust.

1.2 The policies apply to stand-alone personal computers with dial-up modems as well as those attached to networks.

2 Specific policy

2.1 Trust property.

2.1.1 As a work enhancement tool the Trust encourages the business use of secure electronic communications (voice mail, e-mail, text messages and fax).

2.1.2 Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of the Trust, and are not the property of users of the electronic communications services.

2.2 Authorised usage.

2.2.1 The Trust electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as:

(a) It does not consume more than a trivial amount of resources.
(b) It does not interfere with staff productivity.
(c) It does not pre-empt any business activity.

2.2.2 Users are forbidden from using private Internet based mail accounts on Trust Network or personal computers.

2.2.3 Users with both a Trust email account and an email account with the University MUST, in order to comply with Caldicott Guidelines and the Data Protection Act 1998, use the Trust NHS account for all Trust business.

2.2.4 Patient identifiable information should never be transferred to University email accounts.

2.2.5 The Trust will provide email accounts for all staff with genuine requirements, in accordance with the I M& T security policy.

2.2.6 Users are forbidden from using The Trust electronic communications systems for charitable endeavours, private business activities, or amusement/entertainment purposes unless expressly approved by the Trust Chief Executive or his representative.

2.2.7 Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

2.2.8 With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of a department head has been obtained.

3 Patient Requests for email or other electronic correspondence

Patients may request to receive correspondence by email or text messaging. The patient's request to receive clinical and other personal information via email, or other electronic forms, must be recorded in the patient record. The patient must be informed that responsibility for the confidentiality of the received correspondence rests with them and their personal communication service provider (email or text messaging).

4 User separation.

4.1 The Trust staff and authorised contractors have unique usernames and passwords to access the e-mail system.

5 User accountability.

5.1 Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to responsibility for actions the other party takes with the password.

(a) Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored.

(b) If users need to share computer resident data, they should utilise message-forwarding facilities, public directories on local area network servers, and other authorised information-sharing mechanisms.

(c) To prevent unauthorised parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities).

6 No default protection.

6.1 Employees are reminded that Newcastle-upon-Tyne Hospitals NHS Foundation Trust electronic communications systems are not encrypted by default.

6.2 No sensitive personal identifiable information should be sent outside the boundaries of NHS mail accounts or other specified authorised secure services.

7 Respecting privacy rights.

7.1 Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. The Trust is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

7.2 However, The Trust also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

8 No guaranteed message privacy.

8.1 The Trust cannot guarantee that electronic communications will be private.
8.2 Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

9 Regular message monitoring.

9.1 It is the policy of the Trust NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities.
9.2 Users should structure their electronic communications in recognition of the fact that The Trust will from time to time examine the content of electronic communications.

10 Incidental disclosure.

10.1 It may be necessary for IT staff to review the content of an individual employee's communications during the course of problem resolution.
10.2 IT staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels (senior member of staff, head of department).

11 Message forwarding.

11.1 Recognising that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages.
11.2 Trust sensitive information must not be forwarded to any party outside The Trust without the prior approval of a departmental head or the Trust Chief Executive. Blanket forwarding of messages to parties outside The Trust is prohibited unless the prior permission of the chief executive has been obtained.

12 Trust Webmail.

12.1 Users who have access to the Trust's web based email service must ensure that they DO NOT;

- Leave the PC being used to access the web mail logged in.
- Save any Trust documents to the hard drive of the machine being used.

- Do not allow non Trust staff access to their mail account

13 Retention and purging of electronic messages.

13.1 E-mail should be used as a form of communication. Mailboxes should not be used for filing information that has value to the Trust.

13.2 Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. Not only will this increase scarce storage space; it will also simplify record management and related activities. If The Trust is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the chief executive or his designated representative has communicated that it is legal to do so.

14 Messages essentially fall into three main categories.

14.1 Clinical messages.

All clinical messages are to be either deleted as soon as practicable or stored in an electronic file system. Data stored in this way is to be retained in accordance with the Trust Retention and Disposal policy for health records. Until the development of an electronic patient record has been achieved, hard copies of all clinical messages, where appropriate, are to be added to the relevant patient's notes. It is the responsibility of the originator of the email to ensure that the email is stored in the relevant record system.* If the originator is external to the Trust then the recipient must store the record accordingly.

14.2 Business messages.

In accordance with the Freedom of Information Act, and with effect from January 2005, records of business decisions taken by Trust employees may be made available to members of the public on request. This includes documents or decisions made by e-mail. Messages of this kind are to be kept for the duration of the project and either stored in an electronic folder (which pertains to the subject matter) or a hard copy should be taken and kept in the relevant file for the period of the retention stated in the NHS Records Retention Schedules. The originator of the email is responsible for storing the record accordingly.*

14.3 Personal messages

All personal messages are to be deleted as soon as they have been read.

14.4 Other messages

All remaining messages are to be reviewed weekly and deleted if actioned.

* Note that a response to an email that changes the clinical or business record must also be retained in the relevant filing system.

15 Responsibilities.

15.1 As defined below, the Trust groups and staff members responsible for electronic mail security have been designated in order to establish a clear line of authority and responsibility.

15.2 IT must maintain e-mail security policies and standards and provide technical guidance on e-mail security to all Trust staff.

15.3 IT staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Business Managers and Department Heads must ensure that their staffs are in compliance with the personal computer security policy established in this document. IT staff must also provide administrative support and technical guidance to management on matters related to e-mail security.

15.4 The Trust departmental heads must ensure that: Employees under their supervision implement e-mail security measures as defined in this policy.

16 Contact point.

16.1 Questions about this policy may be directed to the I.T Security Officer. Via Helpdesk Tel Ext 25910

Disciplinary process.

Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.

17 Review.

The Personnel Manager, in conjunction with the Head of IM&T, is responsible for the review and amendment of this policy.