Northern Ireland Ambulance Service
Health and Social Care Trust

EMAIL POLICY

Title:	Email Policy		
Purpose of Policy:	The purpose of this policy is to ensure the proper use of the Trust's emails system and make users aware of what the Northern Ireland Ambulance Service Health and Social Care Trust deems as an acceptable use of the email system.		
Directorate Responsible for Policy:	Finance and IT Directorate		
Name and Title of Author:	Mr Paddy Dornan, IT Manager Miss Alison Vitty, Corporate Manager		
Staff Side Consultation	YES. Via HR Joint Working Group – 10 September 2009 Minor amendments made (Point 3.3)		
Equality Screened:	YES		
Date Presented to:	ICT Steering Group	1 June 2009	
	Comments	Approved.	
	Trust Board	24 September 2009	
Publication Date:	01/10/2009	Review:	01/10/2012
Version:	NIAS/TW/IG/10 v1		
(01) October 2009	No previous document to supersede.		
(02)			
(03)			
(04)			

Circulation List:

This Policy was circulated to the following groups for consultation.

- Staffside (via HR Joint Working Group)
- Executive Directors and Senior Managers (1 June 2009)

Following approval, this policy document was circulated to the following staff and groups of staff.

- All Trust Staff
- Trust Internet/Intranet Site

1.0 EMAIL POLICY

1.1 Introduction

This document defines the Email Policy to be applied throughout the Northern Ireland Ambulance Service Health and Social Care Trust and has been developed to ensure that all staff are aware of acceptable and unacceptable use of its email systems.

1.2 Policy Statement

The purpose of this Policy is to ensure that emails are managed effectively throughout the Trust and with due regard to specified legislation, professional principles and guidelines.

This policy applies to all emails created, received or maintained by staff in the Trust in course of carrying out their duties.

Compliance with this policy will ensure that the Trust can provide evidence of performance and demonstrate accountability, as well as providing information about its decisions and activities.

1.3 Purpose and Scope of Policy

The policy is intended to detail the rules of conduct for all staff of the Trust who use email and related services. The Email Policy applies to the use, for the purpose of sending or receiving email messages and attachments of any IT facilities including hardware, software and networks provided by the Trust.

The policy is applicable to all members of the Trust including staff, agency workers and other authorised users of Trust Information Technology (IT) facilities.

Only authorised users of the Trust computer systems are entitled to use email facilities.

2.0 RESPONSIBILITES

2.1 Responsibilities for all Staff and Non-Executive Directors

All staff and Non-Executive Directors are obliged to adhere to this Policy. A failure to adhere to this Policy and its associated procedures may result in disciplinary action. All users of the email system are responsible for ensuring they are acting in compliance with the legal and acceptable use conditions stated at 4.0 below.

Managers at all levels are responsible for ensuring that the staff for whom they are responsible, are aware and adhere to this Policy. They are also responsible for ensuring staff are updated with regard to any changes in this Policy.

2.2 The IT Manager is accountable to the Director of Finance and ICT for the co-ordination and management of the email usage within the Trust. The IT Manager will oversee the implementation of the Policy on behalf of the Director of Finance and ICT. The IT Manager will establish systems and procedures that will support the implementation of this Policy. The IT Manager is also responsible for dealing with complaints regarding email usage and in first instance, for dealing with breaches of the conditions of this policy.

2.3 The IT Department is responsible for the administration of user email accounts and for the provision of a reliable and effective email system.

2.4 The IT Manager is responsible for the maintenance and review of this Policy.

3.0 <u>Principles of Email Provision</u>

3.1 The Trust provides email facilities to authorised users for purposes of approved business activities and administration. Limited personal use is allowed under certain conditions.

3.2 Email cannot be assumed to be a secure medium and **where possible** should not be used for the transmission and/or storage of confidential data without suitable encryption.

3.3 Account holders must not allow any other person to access their accounts. In cases of unexpected absence eg sickness, a Line Manager can request access to an employee’s email account but for specific business purposes only and which will be tightly monitored. Such access must be authorised by a Band 7 or above member of staff (within the Line Management structure of account holder) and clearly state the reason and purpose for same. This request should then be forwarded to the IT Department for consideration. The IT Manager will liaise with the Corporate Manager on same. Consideration of the request to access the account will include how long the staff member is off for; the timeframe to deal with the request etc. Access to any accounts will be recorded and staff will be advised if the account has been accessed and for what legitimate business use. Local processes should be in place to minimise this being required.

4.0 **Standards Use – Compliance with Legislation**

Acceptable Use

4.1 The Trust's main purpose in providing IT facilities for email is to support the purpose of approved business activities and administration.

4.2 Users are responsible for the handling of received email messages and attachments.

4.3 Users should use their email storage areas responsibility, regularly clearing folders, archiving and saving into shared network folders, where appropriate, to ensure compliance with information governance requirements.

Staff should be aware that when they are leaving their current position, they will be asked to complete a checklist by their Manager which will prompt the leaver to take adequate measures to either file, destroy or transfer the information which they have been responsible for in their current job and in line with legislative principles of Freedom of Information 2000 and the Data Protection Act 1998.

Unacceptable Use

4.4 IT facilities provided by the Trust should not be abused. An absolute definition of abuse is difficult to achieve but includes (but is not necessarily limited to):

(i) Creation or transmission of material which brings the Trust into disrepute;
(ii) Creation or transmission of material that is illegal;
(iii) The transmission of unsolicited commercial or advertising material, chain letters or other junk mail of any kind;
(iv) The authorised transmission to a third party of confidential material concerning the activities of the Trust;
(v) The transmission of material such that this infringes copyright concerning the activities of the Trust;
(vi) Activities that unreasonably waste staff effort or networked resources or activities that unreasonably serve to deny service to other users;
(vii) Activities that corrupt or destroy other users' data or disrupt the work of other users;
(viii) Unreasonable or excessive personal use;
(ix) Creation or transmission of any offensive, obscene or indecent images, data or other material;
(x) Creation or transmission of material whish is designed or likely to cause annoyance, inconvenience or anxiety;

(xi) Creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, martial status, disability, political or religious beliefs;

(xii) Creation or transmission of defamatory material or material that includes claims of a deceptive nature;

(xiii) Activities that violate the privacy of others or unfairly criticise or misrepresent others; this includes copying distribution to other individuals;

(xiv) Creation or transmission of anonymous messages or deliberating forging messages or email header information ie without clear identification of the sender;

(xv) The unauthorised provision of access to the Trust's services and facilities by third parties.

5.0 Personal Use

5.1 All e-mails relating to the conduct of the business transactions of the Trust would be regarded as work e-mails and are not personal. However, any e-mail not related to the business of the Trust would be considered personal.

The Trust's computing regulations allow small-scale personal use of Trust e-mail facilities (as a privilege and not a right). The Trust accepts no responsibility whatsoever arising from the use of Trust systems for personal use.

To limit the circumstances in which it becomes necessary for Trust staff (e.g IT staff) to examine your personal e-mails, you are advised to set up a folder called, "Personal" within your e-mail account. All sent and received personal e-mails should either be deleted or stored in this folder.

Ensure that you only deal with genuinely personal material in this way; if there is reason to believe that work-related information has been marked as "personal" to evade data protection or freedom of information requirements, we may have to access all your personal e-mails to identify those that are really work related.

For personal use of email, the following should be adhered to (this is not an exhaustive list):

(i) A level of use that is not detrimental to the main purpose for which the facilities are provided. Priority must be given to use of resources for the main purpose for which they are provided;

(ii) Personal usage must not be of a commercial or profit making nature, or for any other form of personal financial gain;

(iii) Not be of a nature that competes with the Trust business.
(iv) Not be connected with any use or application that conflicts with an employee's obligations to the Trust as their employer.

6.0 Monitoring of Email Usage

6.1 In line with legislative requirements of the Regulation of Investigatory Powers Act 2000, it makes it an offence for the Trust to intentionally, or without lawful authority, intercept communications without the express or implied consent of both the sender and recipient of the communication.

6.2 However, there are permitted exceptions to that principle that interception without consent is unlawful. These include:

(i) Ensuring the effective operation of the system, for instance:

- Scanning for viruses and other potentially harmful attachments;
- Monitoring email storage usage;
- Forwarding messages to the correct address;
- Eliminating spam.

(ii) Investigating or detecting unauthorised use.
(iii) Checking whether communication is relevant to the Trust's business.
(iv) Ascertaining compliance with legislative and/or regulatory practices or procedures e.g. Freedom of Information Act 2000, Data Protection Act 1998;
(v) Preventing or detecting crime or in interests of national security. This must be authorised by the Director of Finance and IT and only in instances where there is reasonable suspicion of criminal misuse or on the request of PSNI or specified public bodies.
(vi) Most of the monitoring carried out by the IT Department is to ensure effective operation and is done automatically at the server level. This is no routine monitoring of the content of users' email by IT staff.

7.0 Breaches of the Email Policy

7.1 Complaints about usage and notification of alleged breaches of the rules and regulations relating to network use should be made, in the first instance, to the IT Manager.

7.2 If a breach is suspected, authority is vested in the Director of Finance and IT to suspend temporarily access to email accounts by any user suspected, pending full investigation.

7.3 Investigations that involve accessing a user's email account should be referred to the Trust's Director of Finance and ICT for authorisation.

7.4 Any disciplinary action taken will be follow the Trust's agreed Disciplinary Procedure for staff.

8.0 **Review**

8.1 This policy will be reviewed every three years or at times considered necessary as a result of operational changes, legislative changes, risk assessments or when breaches in security have occurred.

Related Documentation:

This policy should be read in conjunction with:

ICT Strategy 2009/10 to 2014
ICT Security Policy
Records Management Strategy 2006-2009
Records Management Policy and associated information sheets
Data Protection Policy 1998 and associated procedures
Freedom of Information Policy 2000 and associated procedures
Risk Management Strategy
Password Policy
Internet Policy

Signed: ________________________
Liam McIvor (Mr)
CHIEF EXECUTIVE