Northern Ireland Ambulance Service
Health and Social Care Trust

POLICY ON THE USE OF THE INTERNET

Title:	Policy on the Use of the Internet		
Purpose of Policy:	This policy document tells you how you should use the Trust's internet facility. It outlines your personal responsibilities and informs what you must and must not do.		
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	HR Joint Working Group 10 September 2009. No Comments		
Equality Screened:	YES		
Date Presented to:	ICT Steering Group	1 June 2009.	
	Comments	No comments	
	Trust Board	24 September 2009	
Publication Date:	01/10/2009	Review:	01/10/2012
Version:	NIAS/TW/IG/6 v1		
(01) October 2009	No previous document to supersede. Information on same had previously been detailed in ICT Security Policy.		
(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 (during week of 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

Policy on the Use of the Internet

1.0 Policy Statement

The Northern Ireland Ambulance Service Health and Social Care Trust will ensure all users of Trust provided internet facilities are aware of the acceptable use of such facilities.

2.0 Purpose

This policy document tells you how you should use the Trust's internet facility. It outlines your personal responsibilities and informs what you must and must not do.

The internet facility is made available for the business purposes of the Trust. A certain amount of personal use is permitted in accordance with the statements contained within this Policy.

It is recognised that it is impossible to define precise rules covering all available internet activities. The spirit of the policy needs to be adhered to in order to maximise productive use of the internet.

This policy updates and replaces all locally agreed Internet usage policies.

3.0 Scope

This Internet Acceptable Usage Policy applies to, but is not limited to all Northern Ireland Ambulance Health and Social Care Workers, contractual third parties and agents of the Trust who access the Trust's Internet service and IT equipment.

4.0 Definition

This Internet Acceptable Usage Policy should be applied at all times when using the Trust's provided Internet facility. This includes access via any device including a desktop computer or a mobile device or remote access via home working facilities provided by the Trust.

5.0 Risks

The Trust recognises that there are risks associated with users accessing and handling information in order to conduct official Trust business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents;
- The loss of direct control of user access to information systems and facilities etc

Non-compliance with this policy could have a significant effect on the efficient operation of the Trust and may result in financial loss and an inability to provide necessary services to patients and our stakeholders.

6.0 Applying the Policy

6.1 What is the Purpose of Providing the Internet Service?

The internet service is primarily provided to give Trust employees:

- Access to information that is pertinent to fulfilling the Trust's business obligations.
- The capability to post updates to Trust owned and/or maintained web sites.
- An electronic commerce facility (for limited use and procurement purposes).

6.2 What You Should Use Your Trust Internet Account For

The Trust Internet account should be used in accordance with this policy to access anything in pursuance of your work including:

- Access to and/or provision of information;
- Research.

6.3 Personal Use of the Trust's Internet Service

At the discretion of your Line Manager and provided it does not interfere with your work, the Trust permits personal use of the Internet in your own time (for example during your lunch-break for a limited period of time).

The Trust is not, however, responsible for any personal transactions you enter into - for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep the Trust protected against, any claims, damages, losses or the like which might arise from your transaction - for example in relation to payment for the items or any personal injury or damage to property they might cause.

If you purchase personal goods or services via the Trust's Internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Trust. However, it is preferable that this does not occur.

If used, you should ensure that personal goods and services purchased are not delivered to Trust property. Rather, they should be delivered to your home or other personal address.

If you are in any doubt about how you may make personal use of the Trust's Internet Service you are advised not to do so.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Trust and may be accessed at any time by the Trust to ensure compliance with all its statutory, regulatory and internal policy requirements.

6.4 Internet Account Management, Security and Monitoring

The Trust will provide a secure logon-id and password facility for your Internet account. The Trust's IT Department is responsible for the technical management of this account.

You are responsible for the security provided by your Internet account log-on ID and password. Only you should know your log-on ID and password and you should be the only person who uses your Internet account.

The provision of Internet access is owned by the Trust and all access is recorded, logged and interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted by lack of capacity.
- The filtering system monitors and records all access for reports that may be produced for line managers and auditors on request.

6.5 Things You Must Not Do

Access to the following categories of websites is blocked using a URL filtering system including such areas as:

- Harmful and stealth;
- Personal Business i.e. hotmail accounts;
- Time Wasting;
- Adult and Nudity;
- Advertising;
- Banking and Investment;
- Criminal and Undesirable;
- Discussions and Forums;
- Free time and entertainment;
- Gambling;
- General exclusions;;
- Messaging and communications;
- Violence, Hatred and Profanity;
- Dating;
- Radio stations;
- Games.

However, on limited occasions access to sites is allowed for a valid and lawful business processing reason and which is monitored by the IT Department.

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must **not** use your Internet account to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Run a private business.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive. *"Unsuitable"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and material that is against the rules, essence and spirit of this and other Trust policies.

6.6 Your Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.
- Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- Know that you may only use the Trust's Internet facility within the terms described herein.

6.7 Line Manager's Responsibilities

It is the responsibility of Line Managers to ensure that the use of the Internet facility:

- Within an employees work time is relevant to and appropriate to the Trust's business and within the context of the users responsibilities.
- Within an employees own time is subject to the rules contained within this document.

7.0 Policy Compliance

7.1 If any user is found to have breached this policy, they may be subject to Trust's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Untoward Incidents

7.2 The nature of the Internet is such that it may not always be possible to avoid accessing material which is prohibited by terms of this policy.

Users who are placed in this position should contact the IT Helpdesk immediately so that their systems can be cleaned. Accidental access will not result in disciplinary action but failure to report may do so.

7.3 Users who believe that the internet systems are being used in a way which they regard as being offensive, potentially illegal or which otherwise appears to contravene this policy or statutory requirement should contact the Trust's IT Manager.

7.4 If you do not understand the implications of this policy or how it may apply to you, seek advice from the IT Manager or Corporate Manager.

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 2008 and associated procedures
Freedom of Information Policy 2000 and associated procedures
Email Policy
Passwords Policy
Risk Management Strategy

Signed: _____

Liam McIvor (Mr)
CHIEF EXECUTIVE