Northern Ireland Ambulance Service
Health and Social Care Trust

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SECURITY POLICY

Title:	Information and Communications Technology (ICT) Policy		
Purpose of Policy:	To ensure that Trust staff understand the principles of ICT Security and their responsibilities		
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	Minor amendments made re: lockable windows	
	Trust Board	24 September 2009	
Publication Date:	01/10/2009	Review:	01/01/2016
Version:	NIAS/TW/IG/7 v3		
(01) 2004	This policy has now been superseded and should be removed from all Directorate areas.		
(02) October 2009	The policy has been completed re-structured to take consideration of information governance requirements. Further policies have now also been separately developed to give clear guidance on management of email use, internet use and password management.		
(03) January 2016	The Policy has been reviewed by ICT Manager to ensure legislative and good practice guidance has been adhered to.		
(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

1.0 Introduction

The Northern Ireland Ambulance Service Health and Social Care Trust (the "Trust") are managing a significant investment in the use of Information and Communications Technology (ICT). In many areas of the organisation, the work and use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level that is appropriate for the Trust's needs.

It is also essential that all Trust ICT systems are protected to an adequate level from business risks. Such risks include accidental data change or release, malicious user damage, fraud, theft, failure and natural disaster. It is important that a consistent approach is adopted to safeguard the Trust's information in the same way other tangible assets are secured, with due regard to the highly sensitive nature of some information held on both electronic and manual systems.

2.0 Scope

This ICT Security Policy applies to:

- ICT systems belonging to, or under the control of, NIAS HSC Trust;
- **All** users of our WiFi wireless communication services and to all our internet related services.
- Information stored, or in use, on NIAS HSC Trust systems;
- Information in transit across the Trust's voice or data networks;
- Control of information leaving the Trust;
- Information access resources;
- **All** parties who have access to, or use of ICT systems and information belonging to, or under the control of, NIAS HSC Trust.

3.0 Policy Statement

It is the duty of each Health and Social Care (HSC) body to establish and keep in place arrangements for the purpose of monitoring and improving the quality of healthcare provided by and for that body. The Trust has developed this ICT Security Policy to:

3.1 Provide direction and support for ICT security in accordance with business requirements, regulations and legal requirements;

3.2 State the responsibilities of staff, partners, contractors and any other individual or organisation having access to the Council's ICT systems;

3.3 State management intent to support the goals and principles of security in line with business strategy and objectives;

3.4 Provide a framework by which the confidentiality, integrity and availability of ICT resources can be maintained;

3.5 Optimise the management of risks, by preventing and minimising the impact of ICT security incidents;

3.6 Ensure that all breaches of ICT security are reported, investigated and appropriate action taken where required;

3.7 Ensure that supporting ICT security policies and procedures are regularly reviewed to ensure continued good practices and protection against new threats;

3.8 Ensure ICT information security requirements are regularly communicated to all relevant parties.

4.0 **Policy Objective**

4.1 To ensure that equipment, data and staff are adequately protected against any action that could adversely affect the Trust. These events will include accidents as well as behaviour deliberately designed to cause difficulties. Adherence to this policy and related policies and procedures will ensure that that risk of such occurrences is minimised.

4.2 To ensure that all staff are aware of and fully comply with all relevant legislation;

4.3 To create and maintain within the Trust a level of awareness of the need for ICT security to be integral part of the day to day business, so that all staff understand the need for ICT security and their own responsibilities in this respect.

5.0 **Roles and Responsibilities**

5.1 All staff are required to adhere to the ICT Security Policy and related policies and procedures. The sections below detail specific responsibilities for all staff and specific staff groups.

5.1.1 **All Staff**

All members of staff have a responsibility to:

General

- Ensure that no breach of ICT security results from their actions;
- Bring to their Manager's attention areas of concern regarding information security and report appropriately, as required under the Trust's Risk Management Strategy;
- Abide by the relevant legislation relating to ICT security.

Equipment Disposal

- Ensure the IT Helpdesk are informed of any ICT equipment that needs to be disposed of. Under no circumstances should staff pass on or dispose of equipment themselves.
- Reformat or rewrite or physically destroy all removable media before disposal to guard against unauthorised access to personal data. Staff should contact the IT Department on how to manage this.

Physical Security

- Ensure doors and windows are closed or locked (where appropriate) and secure when the area is left unattended in areas where ICT equipment is in use.
- Ensure, where possible, all portable equipment is secured when not in use.
- Do not leave equipment or removable media unattended when travelling.
- Do not leave portable media e.g. USB sticks, external hard drives, DVDs inside portable computers when travelling in case of theft.
- Ensure that unattended PCs/laptops have appropriate protection e.g. log off, lock screens or use password protection.
- Ensure all portable equipment i.e. laptops are encrypted and encryption software is running effectively. Staff should seek advice from the IT Department on how to manage this.

Information Security

- Store information on networked drives that are subject to authorisation and access controls.
- Ensure that all personal information is transferred in line with the standards set in associated policies and procedures.

5.1.2 **Line Managers**

Have a responsibility to:

General

- Ensure that all current, new and temporary staff are instructed in their security responsibilities and work in a manner consistent with the ICT Security Policy.
- Ensure that all their staff using computer systems/media are trained in their use.
- Ensure that the IT Helpdesk are notified through completion of appropriate paperwork of new and leaving employees to allow access rights to be appropriately established from effective dates and leaving employees access to be revoked. New users will not be assigned log-on credentials without completed user request forms from their line manager.
- Investigate and take relevant action on any potential breaches of this policy supported by the Risk Manager and other appropriate personnel in line with existing risk management strategy.

Information Security

- Ensure that no unauthorised staff are allowed to access any of the Trust's computer systems or information stores, as such access would compromise information integrity.
- Ensure that non-Trust employed staff e.g. contractors, students, temporary agency staff etc have signed the confidentiality code of conduct for non-Trust employed staff before accessing ICT equipment.
- Determine which individuals are to be given authority to access specific information; levels of access to specific systems should be based on job function, independent of status.
- Decide whether it is appropriate for their staff to use private equipment e.g. PDAs, USB memory sticks. This will include considering whether it is needed to carry out their duties and whether it may pose a confidentiality or security risk.
- Ensure that removable media used by their staff is disposed of securely, seeking guidance from the IT Department where appropriate.
- Ensure that the Checklist for Staff is completed before an employee leaves a job; that relevant accounts are closed and equipment returned e.g. mobile phones, PDAs, laptops etc

5.1.3 **Finance and ICT Directorate**

The Finance and ICT Directorate is managed by the Director of Finance and ICT. This area of management includes the IT Department and Information Department who are dedicated to the role of information

governance within the Trust and whose responsibility it is to develop and implement ICT security across the Trust.

To ensure ICT security, the IT Department has a responsibility to:

General

- Monitor and report on the state of ICT security within the Trust.
- Ensure that ICT Security Policy is implemented throughout the Trust.
- Develop and enforce detailed procedures to maintain security.
- Ensure that Trust personnel are aware of their responsibilities and accountability for information security.
- Provide advice on information security when required.
- Assess the impact of ICT provision of any major disruption and invoke appropriate action as per the Business Continuity Plan.
- Implement adequate processes to ensure that third parties with whom the Trust contracts are subject to, and comply with, information security requirements.

Information Security

- Monitor for actual or potential information security breaches.
- Develop procedures to investigate and report ICT security issues.
- Understand the risk to the computer assets and the information that is held on them.
- Implement specific measures where personal information is being transferred whether manually or electronically e.g. using portable computers, USB. This must include data encryption procedures.
- Ensure access controls are established and maintained for all staff to ensure appropriate access to information.
- Commission penetration testing to ensure network security.
- Ensure back-up procedures are established and maintained.

Physical Security

- Deploy appropriate security measures to reduce the threat and to reduce the impact of a threat that materialises.
- Ensure that new information systems provide an adequate level of security and do not compromise the existing infrastructure.
- Ensure appropriate revision of antivirus software and patches are installed on all servers and PCs.
- Produce and maintain an ICT asset register for software and hardware used by all Trust staff.
- Ensure server rooms are restricted to appropriate staff members.

- Ensure that all critical equipment is protected from power supply failures and bursts using Uninterruptable Power Supplies (UPS) and UPS are tested on a regular basis.
- Ensure that PCs, servers and other appropriate hardware are disposed of security in accordance with disposal schedule.

5.1.4 **Information Governance Steering Group**

The Trust is committed to the ongoing development and review of ICT Policies, procedures and guidelines to manage the risk of emerging threats to its systems and services. This work will be coordinated by the Information Governance Steering Group chaired by the Director of Finance and ICT.

The IG Steering Group has responsibility for developing and implementing ICT Security Policy and associated procedures and ensuring the Trust meet national and legislative requirements in relation to ICT Security. Other specific areas relating to information security including data protection, confidentiality and data quality are also overseen by this Group.

5.1.5 **Human Resources Directorate**

Has a responsibility to:

- Ensure necessary screening of staff is carried out through the recruitment process;
- Ensure every contract references employees' responsibilities with regard to information security and make it clear that employees are required to comply with the Trust's policies on information governance matters.
- Ensure that staffs are given access to relevant policies and procedures.
- To ensure that the Checklist for Staff is completed before an employee leaves a job.

6.0 Application

6.1 For the purposes of this document, the terms ICT/ICT system, ICT data or ICT user are defined as follows:

- **ICT** means any device or automatic storing and processing of data and includes mainframe computer, minicomputer, microcomputer, personal computer (whether hand-held laptop, portable, stand-alone, network or attached to a main server), workstation, word processing system, desktop publishing system, office automation system; messaging system or any other similar device;

- **ICT data** means any information stored and processed by ICT and includes programs, texts, picture and sound;
- **ICT user** applies to any Trust employee or other authorised person who uses the Trust's ICT system and/or data.

7.0 Definitions

7.1 **Encryption** is the process of converting information into a form unintelligible to anyone except holders of a specific key or password.

7.2 **External hard drive** sits outside the main computer in its own enclosure. This portable encasement allows the user to store information on a hard drive that is not part of the computer, but is connected via a high-speed interface cable normally a USB or fire wall.

7.3 **Hardware** in IT is a physical device such as a VDU or printer.

7.4 **Patches** are updates on computers, such as anti-virus, to ensure that the program is up to date or to fix a bug within a program.

7.5 **Mobile Device**, refers to a portable device that has several features including an address book, contacts list, calendar, memo and notepad e.g. Laptop, Ipad, smartphone etc.

7.6 **Removable Media** is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. floppy discs, CDs/DVDs, USB flash memory sticks or pens.

7.7 **Software** are programs that run on a computer e.g. word processing software, spreadsheets etc.

7.8 **USB** (Universal Serial Bus) or Port connection, that are universally compatible with many types of devices such as wireless, printers, memory sticks etc.

7.9 **USB Memory sticks** are devices with flash memory card formats. These devices come in many sizes and are generally used for storage of data.

8.0 Legislation

8.1 The Trust is obliged to abide by all relevant UK and European Union legislation in relation to information security and ensure that all of its information systems adhere to this legislation. It must also ensure that individual responsibilities for meeting these requirements are clearly defined in local system documentation. Legislation of relevance to information security and monitoring includes (this is not an exhaustive list):

- The Data Protection Act 1998
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1999
- The Health and Safety at Work (NI) Order 1978
- The Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- The Electronic Communications Act (2000)
- Privacy and Electronic Communications Regulations (2003)
- Fraud Act 2006

9.0 Assets

9.1 There are six major categories of information assets including information, software, physical (including hardware), services, people and less tangible assets such as reputation and image of the Trust. The key assets that this policy applies to are information hardware and software. Co-ordination with the Trust's financial system is also of key importance.

9.2 Asset Register

A complete ICT register which will include key hardware and software will be maintained by the IT Department for all health information assets. Procurement of new assets must be recorded in the asset register and allocated to the appropriate owner. Disposal of assets or the reassignment of assets must be recorded in the asset register.

9.3 Authorised Hardware and Software

9.3.1 Users requiring equipment to carry out authorised tasks are to apply for equipment and funding through Directorate Heads and in line with financial policy and procedures. With the introduction of any new project across the Trust, the ICT requirements should be considered from the outset, embedded within the project management environment.
Purchase of this equipment will then be carried out centrally by the IT Department following the release of the appropriate Business Case. This ensures that equipment purchased is compatible with existing systems.

9.3.2 Any new software must be authorised by the IT Department. Unauthorised software must not be used on Trust equipment or network.

9.3.3 If the Trust has purchased software, the IT Department will retain the purchase licence, should any reinstall be necessary.

9.3.4 The user must not modify the equipment. Such modifications that are required to ensure the efficiency of the PC will be provided and installed by IT staff (within budgetary constraints). Modifications include:

- Software installations unless delegated to the user by a member of the IT Department;
- Hardware and software upgrades.

9.4 **Use of Private Equipment**

9.4.1 Private equipment will not be used for the purpose of carrying out Trust business without prior permission from the individual's Line Manager. This private equipment may include laptops, PDAs, USB memory sticks and external hard drives.

9.4.2 It will then be the responsibility of the Line Manager to decide if it is necessary for the person to carry out their duties or whether it may pose a confidentiality or security risk. If needed, the IT Department can be contacted for further support.

9.5 **Maintenance**

9.5.1 The IT Department maintains ICT hardware and software for the Trust. A staff member cannot authorise any maintenance to be carried out by another agency.

9.6 **Information Storage and Back-Up**

9.6.1 Users are responsible for ensuring their information is saved appropriately and subject to regular back-up. Where a user has network access, all information should be saved to their network drive which is automatically backed up by the IT Department.

9.6.2 All information should be managed in accordance with supporting information governance policies and procedures.

10.0 Incident and Risks

10.1 All risks and incidents relating to ICT Security must be reported using the Trust's standard procedure for risk and incident reporting.

10.2 Breaches of this Policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to NIAS assets, or an event which is in breach of NIAS security procedures and policies.

All NIAS employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Trust's standard procedure for risk and incident reporting. This obligation also extends to any external organisation contracted to support or access the Information Systems of NIAS.

10.3 Reporting of risks and incidents is important to ensure that appropriate action is taken so that risks/incidents do not reoccur and to learn from them. No consecutive action can be taken if the Trust is not notified when things go wrong or there is a near miss.

11.0 Access Control

11.1 Access to business and confidential information must be controlled appropriately. All employees are entitled to use the network and office applications provided by the IT Department provided it is applicable to their particular role.

12.0 User Access Management

12.1 The Trust have formal registration and de-registration procedures which covers networked and non-networked sites, granting and managing access to network directories and systems. All users of the Trust's computer network are required to sign the Trust's network authorisation form which will indicate their access needs. The user request form must be countersigned by the user's line manager before submitting it to the IT Department for approval.

13.0 Password Control

13.1 Deliberate sharing of systems access passwords is a criminal offence under the Computer Misuse Act 1990. All staff are required to follow good security practices in the selection and use of passwords and should refer to the Trust's Policy on the Use and Management of Passwords for further guidance.

14.0 Acceptable Use of Email and Internet

14.1 The Trust needs to ensure that all staff are protected against viewing or accessing inappropriate materials. Further guidance is available in the Trust's Email and Internet Policies which have been developed to minimise the risk in relation to email and internet use and advice on best practice in this area. These policies must be read and adhered to by all staff to support ICT security and best practice.

15.0 Remote Access

15.1 Remote access occurs when a user logs onto the Trust network from a location where there is no direct access to the Trust's network e.g. a member of staff remotely accessing the network from home.

15.2 Critical business processes rely on easy and reliable access to clinical and corporate information systems. However remote access is not given as a right and will only be granted on a case by case basis and approval from relevant Executive Director.

16.0 Exchanges of Information and Software

16.1 It is imperative that utmost care is exercised when transferring information, especially information of a confidential nature e.g. staff, patient or service user information. This includes transferring information by telephone (voice and text), email, fax, courier and public mail. Encryption services must be engaged where available.

16.2 Regular exchanges of information outside of the HSC must be governed by an information sharing protocol using the Trust's standard template. Further guidance on this is available from the Trust's Corporate Manager and Information Department in general.

17.0 Systems Development and Maintenance

17.1 The Trust must ensure that security requirements are built into systems from the outset. Suitable controls must be in place to manage the purchase or development of new systems and the enhancement of existing systems, to ensure that information security is not compromised.

Security Requirements of Systems

17.1.1 Any individual responsible for implementing or modifying systems is responsible, in collaboration with the IT Department for ensuring:

- The statements of business requirements for new systems, or enhancements to existing systems specify the security controls required for that system;
- That all modifications to systems are logged and up to date documentation exists for their systems;
- The vendor supplied software used in systems is maintained at a level supported by the suppler, if beneficial to the Trust. Any decision to upgrade must take into account the security of the release;

- That physical or logical access is only provided to suppliers for support purposes when necessary, and must be with management and IT approval;
- That all supplier activity on the system is monitored;
- That copies of data must retain the same levels of security and access controls as the original data.
- That changes to central documentation are completed prior to any upgrade or modification of existing systems, or the introduction of a new system which may have an impact on existing systems.

18.0 **Business Continuity**

18.1 A Business Continuity Plan must exist to allow all critical systems to be maintained and to restore clinical systems in the event of a major disruption to service e.g. through a disaster or security failure.

19.0 **Review**

19.1 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 2016/17-2020 (Draft)
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 and associated information sheets
Passwords Policy
Risk Management Strategy

Signed: _____

Liam McIvor (Mr)
CHIEF EXECUTIVE