



IM&T SECURITY POLICY

Policy Number:	IG 08
Version:	2.0
Ratified by:	SEE PCT Board
Date ratified:	26th March 2009
Name of originator/author:	Paul Cook (Head of Information Governance)
Name of responsible committee/individual:	SEE PCT Integrated Governance Committee
Date issued:	June 2009
Review date:	May 2010
Target audience:	All SEE PCT staff and Contractors

Contents

1.	Introduction and Purpose	Page 3
2.	Duties	Page 3, 4
3.	Definitions	Page 4, 5
4.	Designated Individuals Responsible for Information Security and confidentiality	Page 6
5.	Risk Assessments	Page 6
6.	Access Control to the Network(s) (Via ESSA IT Service)	Page 6, 7
7.	Third Party Access Control to the Network(s)	Page 7
8.	Data and Software Exchange	Page 8
9.	Fault Logging (Via ESSA IT Service)	Page 8
10.	User Responsibilities, Awareness & Training	Page 8
11.	Malicious Software	Page 8
12.	Reporting Security Incidents and Weaknesses	Page 8
13.	Unattended Equipment	Page 8, 9
14.	Working on Home (Personal) PCs	Page 9
15.	Trust IT/Information Governance Department Responsibilities	Page 10, 11
16.	Line Manager's Responsibilities	Page 11
17.	General Responsibilities	Page 11, 12
18.	Computer Misuse Act 1990	Page 12, 13
19.	Validity of this Policy	Page 13
20.	Review of the Policy	Page 13
21.	Monitoring the Policy	Page 13
22.	Appendices	Page 13
23.	References	Page 13
	Appendix 1 – Information security incident reporting procedures	Page 14, 15, 16
	Appendix 2 – IM&T Security Policy Declaration	Page 17

1. Introduction and Purpose

- 1.1 This document defines the IM&T Security Policy for South East Essex Primary Care Trust (the Trust) and applies to all staff and users of the Trust network(s) and IT equipment.
- 1.2 The Policy applies to all business functions and information contained on the network(s), the physical environment and relevant people who support the network(s).
- 1.3 This document sets out the Trust's policy for the protection of the confidentiality, integrity and availability of the network(s) and information held on it.
- 1.4 This document establishes the security responsibilities for all employees of the Trust.
- 1.5 Wilful or negligent disregard of this policy will be investigated and will be treated as a disciplinary offence.

2. Duties

- 2.1 The duty of this policy is to ensure the security of the Trust's network(s) and the information held. The Trust will:
 - 2.1.1 Ensure availability of equipment/data
 - 2.1.2 Ensure that the network(s) is available for users.
 - 2.1.3 Maintain reliability of data
 - 2.1.4 Protect the network(s) from unauthorised or accidental modification ensuring the accuracy and completeness of the Trust's assets.
 - 2.1.5 Maintain confidentiality
 - 2.1.6 Protect assets against unauthorised disclosure.
 - 2.1.7 Provide secure and resilient remote access to information systems.
- 2.2 This policy applies to all network(s) used within the Trust:
 - 2.2.1 The storage, sharing and transmission of non-clinical data and images
 - 2.2.2 The storage, sharing and transmission of clinical data and images
 - 2.2.3 Printing or scanning non-clinical or clinical data or images
 - 2.2.4 The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images
 - 2.2.5 Remote access by mobile users, home workers and Non-NHS staff.
 - 2.2.6 Storage and transportation of data and images on removable media.
- 2.3 This policy does not consider individual systems held on the Network(s). These should have their own System Security Policies including the identification of System Administrator(s) who are responsible for providing access to users.

- 2.4 The overall IT Security Policy for the Trust is described below.
- 2.5 The Trust information network(s) will be available when needed, can be accessed only by authorised users and will contain complete and accurate information. The network(s) must also be able to withstand or recover from threats to its availability, reliability and confidentiality. To satisfy this, the Trust will undertake to, in conjunction with the IT Service Provider,
- 2.5.1 Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
 - 2.5.2 Provide both effective and cost-effective protection that is proportionate with the risks to its network(s) assets.
 - 2.5.3 Implement the Network Security Policy in a consistent, timely and cost effective manner.
 - 2.5.4 Where relevant, the Trust and IT Service Provider will comply with:
 - Copyright, Designs & Patents Act 1988
 - Access to Health Records Act 1990
 - Computer Misuse Act 1990
 - The Data Protection Act 1998
 - The Human Rights Act 1998
 - Electronic Communications Act 2000
 - Regulation of Investigatory Powers Act 2000
 - Freedom of Information Act 2000
 - Health & Social Care Act 2001
 - Environmental Information Regulations Act 2004
 - 2.5.5 To provide secure and resilient remote access to the Trust's information systems.
- 2.6 The Trust and IT Service Provider will comply with other laws and legislation, as appropriate.
- 2.7 The policy must be approved by the Trust's Integrated Governance Committee.

3. Definitions

- 3.1 **IT Service Provider** – The External organisation which supplies the Trust with IM&T services
- 3.2 **IM&T** – Information Management & Technology
- 3.3 **NPfIT** – National Programme for Information Technology
- 3.4 **The Trust** – South East Essex Primary Care Trust (PCT)
- 3.5 **SLA** – Service Level Agreement – The contract between the Trust and the IT Service Provider in which it is clearly defined what the

responsibilities are of both parties with regard to Trust policies and UK / European Laws and also the Priority response definitions for IT Support calls which are monitored and measured by the Trust.

3.6 **Network Assets** – A collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by various means and created to share data, software, and peripherals such as printers, modems, fax machines, internet connections, CD-ROM and back-up tapes, hard disks and other data storage equipment.

3.7 **Information Assets** – (examples below)

Personal/Other Information	Software
<ul style="list-style-type: none"> Databases and data files Back-up and archive data Audit data Paper records and reports 	<ul style="list-style-type: none"> Applications and System Software Data encryption utilities Development and Maintenance tools
System/Process Documentation	Hardware
<ul style="list-style-type: none"> System information and documentation Operations and support procedures Manuals and training materials Contracts and agreements Business continuity plans 	<ul style="list-style-type: none"> Computing hardware including PCs, Laptops, PDA, communications devices e.g. blackberry and removable media
	Miscellaneous
	<ul style="list-style-type: none"> Environmental services eg. power and air-conditioning People skills and experience

3.8 **Removable Media** – Includes back-up tapes, external & removable hard drives, DVD, CD-Rom and Pen Drives (encrypted USB storage devices).

3.9 **Sensitive/person-Identifiable Information (PII)** – Includes; person's name, address, full postcode, and date of birth; pictures, photos, videos, audio tapes or other images of patients; NHS number and local identifier codes and anything that could be used to identify a patient directly or indirectly e.g. rare diseases, drug treatments or statistical analyses which have very small numbers in a small population.

3.10 **Faults** – Examples below (All faults need to be reported to the IT Service Provider helpdesk via email/phone) Examples below;

- Computer not switching on
- Password needs to be changed or reset
- Printer not working
- K: // or I: // drive has disappeared

4. Designated Individuals Responsible for Information Security and Confidentiality

4.1 **David Griffiths** (Director of Finance & Information) – Senior Information Risk Owner (SIRO)

4.1.1 Responsible for the overall management of information security and risk

4.2 **Debbie Fielding** (Director of Strategy & Partnerships) – Caldicott Guardian

4.2.1 Responsible for confidentiality of service-user information and sharing of information

4.3 **Paul Cook** (Head of Information Governance) – Information and Technology Security Officer

4.3.1 Responsible for continued management of information security and confidentiality.

4.3.2 Reports directly to the Senior Information Risk Owner (SIRO)

4.3.3 Responsibility to ensure the organisation follows all legal obligations

4.4 **Peter King** (Head of IT) – Information and Technology Security Officer

4.4.1 Responsible for continued management of information technology security

5. Risk Assessment

5.1 The Trust, in conjunction with the IT Service Provider, will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network(s) that are used to support those business processes, including remote access and use of removable media. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, reliability and availability.

6. Access Control to the Network(s) (Via IT Service Provider)

6.1 Access to the network(s) will be via a secure log-in procedure, designed to minimise the opportunity for unauthorised access.

6.2 Departmental managers must approve user access and send a completed 'New User' form and signed 'User Declaration' (Appendix 2) to the IT Department on (Fax) 01702 313699. The original forms should be kept in employee files by the line manager.

- 6.3 Access rights to the network(s) will be allocated on the requirements of the user's job, rather than on a status basis. The completed 'New User' form should clearly state which shared folders the user needs to have access too.
- 6.4 Access to network(s) folders will only be granted to those folders stated on the 'New User' Form or to corporate (general) folders on the shared drives. Amendments and/or additions to the folder access for any given user should be communicated, by the folder owner, to the IT Service Provider helpdesk via email. The Information and Technology Security Officers will authorise all requests.
- 6.5 Requests for new folders on the shared network(s) drives will only be actioned with the inclusion of a nominated owner who will be responsible for identifying and authorising user access to the folder in the future. New folder requests should be communicated, by the nominated owner, to the IT Service Provider helpdesk via email. The Information and Technology Security Officers will authorise all requests.
- 6.6 Security privileges (i.e. 'superuser' or network administrator rights) to the network(s) will be allocated on the requirements of the user's job, rather than on a status basis.
- 6.7 All users must read this policy and sign the declaration before access is granted. The signed declaration will be stored by the IT Department.
- 6.8 Access will not be granted until the IT Department receives a completed and authorised 'New User' Form and a signed 'User Declaration'.
- 6.9 All users to the network(s) will have their own individual username and password.
- 6.10 Users are responsible for ensuring their password is kept secret (see User Responsibilities).
- 6.11 User access rights will be immediately removed or reviewed for those users who have left the Trust or changed jobs. Line managers must inform the IT Department in writing, using the 'Leaver' form, for staff leaving the organisation.

Note: The 'New User' form and 'Leaver' form can be found on the Staff Intranet, in the IT section.

7. Third Party Access Control to the Network(s)

- 7.1 Third party access to the network(s) will be based on a formal contract that satisfies all necessary Trust security and confidentiality conditions.
- 7.2 All third party access to the network(s) must be logged.

8. Data and Software Exchange

- 8.1 Formal agreements for the exchange of data and/or software between organisations must be established and approved by the Senior Information Risk Owner (SIRO), Head of IT, Head of Information Governance and the Caldicott Guardian.

9. Fault Logging (Via IT Service Provider)

- 9.1 The Head of IT is responsible for ensuring that the IT Service Provider maintains a log of all faults (see definition for examples) on the network(s) and that it is regularly reviewed. A procedure to report faults is provided via the IT Service Provider helpdesk, and the review of countermeasures is contained within the IT Service Provider's SLA.

10. User Responsibilities, Awareness and Training

- 10.1 The Trust will ensure that all users of the network(s) are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.
- 10.2 All users of the network(s) must be made aware of the contents and implications of the IM&T Security Policy.
- 10.3 Irresponsible or improper actions by users will result in disciplinary action(s) and or prosecution.

11. Malicious Software

- 11.1 The Head of IT and IT Service Provider will ensure that measures are in place to detect and protect the network(s) from penetration, viruses or other malicious software.

12. Reporting Security Incidents and Weaknesses

- 12.1 All potential security breaches must be investigated and reported to the Head of IT and/or the Head of Information Governance. Security incidents and weaknesses must be reported in accordance with the requirements of the Trust's Information Security Incident Reporting Procedures. (see Appendix 1)

13. Unattended Equipment

- 13.1 Users must ensure that they protect the network(s) from unauthorised access. They must log off the network(s) when finished working.
- 13.2 Users must ensure that any equipment logged on to the network(s) must be protected if they leave it unattended, even for a short time. Workstations must be locked (Ctrl+Alt+Del) or a (5 minute) screensaver password activated if a workstation is left unattended for a short time.

13.3 Users failing to comply will be subject to disciplinary action.

14. Working on Home (Personal) PCs

- 14.1 It is **not** permissible to use Home PCs for any work that uses confidential/sensitive information/data – this includes Trust, staff and patient information. This presents an unacceptable level of risk to the Trust and to the people that the data relates to, due to theft or information still being accessible once the home PC has been disposed of.
- 14.2 Do not download confidential/sensitive information/data from your NHSmail account onto your home pc.
- 14.3 As a general rule, work which does not contain confidential/sensitive information/data is not a high risk area. For example developing a guidance document like this is a general everyday document that would not put the Trust or anyone at risk by being in the public domain or by having a copy sitting on a home PC.

Risks Associated with Working from Home

By not following the above processes;

- 14.4 You cannot guarantee adherence to the trust's security policy, from members of your family or anyone visiting your home.
- 14.5 You would be unable to guarantee virus protection to the trust's standard.
- 14.6 Even if you deleted any trust data on your home PC, any information deleted can be retrieved from your hard drive by an expert. This would create risks from hackers when you eventually dispose of your PC.
- 14.7 Staff with broadband facilities at home pose an even bigger risk as this is an 'always on' connection, which would require an adequate firewall to protect them from hackers.

In addition;

- 14.8 There is a risk of burglary or fire. This has been built into the risk considerations for your workplace to ensure the protection of information.
- 14.9 Discussing anything seen or heard about a patient outside the trust or practice poses a risk to patient confidentiality– this applies even after ceasing employment with the trust

15. Trust IT / Information Governance Department Responsibilities

- 15.1 Acting as a central point of contact on information security and confidentiality within the organisation, for both staff and external organisations.
- 15.2 Assisting in the formulation of the IM&T Security Policy and related policies.
- 15.3 Produce organisational standards, procedures and guidance on information security and confidentiality matters for approval by the Trust's Integrated Governance Committee.
- 15.4 Liaise with external organisations on information security and confidentiality matters, including representing the organisation on cross-community committees.
- 15.5 Ensuring that appropriate Data Protection Act 1998 notifications are maintained for information stored on the network(s).
- 15.6 Dealing with enquiries, from any source, in relation to the Data Protection Act 1998 and facilitating Subject Access Requests.
- 15.7 Advising users of information systems, applications, networks and their responsibilities under the Data Protection Act 1998, including Subject Access Requests.
- 15.8 Advising the Director of Finance and Information (SIRO) and the IT Programme Director on breaches of the Act and recommended actions.
- 15.9 Encouraging, monitoring and checking compliance with the Data Protection Act 1998.
- 15.10 Liaising with external organisations regarding Data Protection Act 1998 matters.
- 15.11 Promoting awareness and providing guidance and advice related to information security and confidentiality as it applies within the Trust.
- 15.12 Creating, maintaining, giving guidance on and overseeing the implementation of IT security.
- 15.13 Representing the organisation on internal and external committees that relate to IT security.
- 15.14 Providing advice and guidance for Trust staff to ensure that the policy is complied with.
- 15.15 Providing a central point of contact on IT security issues.

- 15.16 Providing advice and guidance for:
- Policy compliance
 - Incident investigation
 - IT security awareness
 - IT security training
 - IT systems accreditation
 - Security of external service provision
 - Contingency planning for IT systems
 - Shared file structure and ownership
- 15.17 The Head of IT is responsible for providing clear authorisation for all remote access and users' level of access.
- 15.18 The IT Service Provider will ensure that user profiles and access controls are implemented in line with agreed levels.
- 15.19 All remote users will be registered by the IT Service Provider and authorised by the Head of IT and Line Manager.
- 15.20 The IT Service Provider and Head of IT will ensure a log is kept for all users with remote access.

16. Line Manager's Responsibilities

- 16.1 Ensuring the security of the network(s), that is information, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- 16.2 Ensuring that their staff are made aware of their security and confidentiality responsibilities.
- 16.3 Ensuring that their staff have had suitable information security training.
- 16.4 Are responsible for, in collaboration with the Head of IT and/or the Head of Information Governance, the day to day management and oversight of removable media used within their work areas, to ensure policies are followed.
- 16.5 To inform the IT Department in writing, using the 'Leaver' form, for staff leaving the organisation.

17. General Responsibilities

- 17.1 All personnel or agents acting for the organisation have a duty to:
- 17.1.1 Safeguard PCT hardware, software and information in their care.
 - 17.1.2 Prevent any malicious software being downloaded onto the organisation's IT systems.
 - 17.1.3 Report on any suspected or actual breaches of information security.

- 17.2 ALL sensitive/person-identifiable information/files saved and/or transported on any media (including those listed below) **MUST** be encrypted (for further information regarding encryption, refer to Head of IT and/or the Head of Information Governance):-
- Hard Drive (C Drive) of desktop
 - Laptop/tablet PCs, Smartphones, PDAs, Blackberries etc.
 - Mobile storage such as; Pen Drives (USB storage devices), external hard drives, CD/DVDs, back-up tapes, etc.
- 17.3 All remote access users are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources.
- 17.4 Remote users must return all relevant equipment when leaving the Trust.
- 17.5 No member of staff is permitted to access, display or download from Internet sites that hold offensive material. Offensive material is defined by the Trust's Equal opportunity and Harassment Policy. Other than instances which demand criminal prosecution, the Trust is the final arbiter on what is or is not offensive material, or what is or not permissible access to and use of Internet and e-mail.
- 17.6 Staff and contractors are not permitted to introduce or use any removable media other than those provided or approved for use by the Information Governance Team.
- 17.7 Removable media may only be used to store and share Trust information that is required for a specific business purpose (not sensitive/person-identifiable information, unless authorised).
- 17.8 When the business purpose has been satisfied, the contents held on the removable media must be removed through a method that makes recovery of data impossible. Alternatively the media and its data should be destroyed and disposed of beyond its potential reuse. A record of the action to remove data should be recorded.
- 17.9 Staff should maintain a record of all removable media taken off site, or brought into/received by the Trust. The record should identify information files involved as well as the media.
- 17.10 Removable media must be protected against loss, damage abuse or misuse when used, where stored and when transported.

18. Computer Misuse Act 1990

- 18.1 Staff should be aware that it is an offence to knowingly use their computers to gain access to unauthorised programs or data. This includes the browsing of information on monitors; downloading data as well as the changing of data or programs by persons unauthorised to do so.

18.2 Should the above be done with the intent to cause a crime (e.g. fraud, selling information), this would also be dealt with as an offense.

18.3 It is an offence to carry out unauthorised modification to data or programs, impair the operation, prevent or hinder access to programs or data held on a Trust computer.

19. Validity of this Policy

19.1 This policy should be reviewed annually under the authority of the Chief Executive. Associated information security standards should be subject to an ongoing development and review programme.

20. Review of this Policy

20.1 This document will be subject to review when any of the following occur:

20.1.1 The adoption of the standards highlights errors and omissions in its content

20.1.2 Where other standards / guidance issued by the Trust conflict with the information contained

20.1.3 Where good practice evolves to the extent that revision would bring about improvement

21. Monitoring the Policy

21.1 The Information Governance Committee (IGC) will monitor the implementation of this policy, its supporting procedures, and subsequent revisions.

22. Appendices

22.1 **Appendix 1** – Information Security Incident Reporting Procedures

22.2 **Appendix 2** – IM&T Security Policy Declaration

23. References

Email Usage Policy
Internet Usage Policy
Mobile Computing and Remote Access Policy
Password Policy
Safe Haven Policy

Appendix 1

INFORMATION SECURITY INCIDENT REPORTING PROCEDURES**1. INTRODUCTION**

- 1.1 Incident reporting plays a major role in helping the organisation maintain a secure working environment. It helps to protect the confidentiality, integrity and availability of the information and systems.
- 1.2 All staff have a responsibility to report security incidents whether deliberate or accidental.

2. What is an Information Security Incident?

- 2.1 A security incident is defined as:
 - 2.2 ***Any actual or potential breach of security which may compromise the confidentiality, integrity or availability of information.***
 - 2.3 The term security incident covers a wide range of events which can vary considerably and it is therefore not possible to detail every single event. However the following list gives examples of the types of security incidents that should be reported:
 - 2.4 An information security incident can be defined as any event that has resulted or could result in:
 - 2.4.1 The disclosure of confidential information to an unauthorised individual
 - 2.4.2 The integrity of a system or data being put at risk
 - 2.4.3 The availability of the system or information being put at risk
 - 2.5 An adverse impact can be defined for example as:
 - 2.5.1 Threat to personal safety or privacy
 - 2.5.2 Legal obligation or penalty
 - 2.5.3 Financial loss
 - 2.5.4 Disruption of Organisational business
 - 2.5.5 An embarrassment to the Organisation
 - 2.6 Examples of security incidents:
 - 2.6.1 Using another user's login id/swipe card
 - 2.6.2 Unauthorised disclosure of information
 - 2.6.3 Leaving confidential / sensitive files out
 - 2.6.4 Theft or loss of IT equipment
 - 2.6.5 Theft or loss of computer media, i.e. floppy disc or memory stick
 - 2.6.6 Accessing a person's record inappropriately e.g. viewing your own health record or family members, neighbours, friends etc.

- 2.6.6 Writing passwords down and not locking them away
- 2.6.7 Identifying that a fax has been sent to the wrong recipient
- 2.6.8 Sending/receiving a sensitive email to/from "all staff" by mistake
- 2.6.9 Giving out or overhearing personally identifiable information over the telephone
- 2.6.10 Positioning of pc screens where information could be viewed by the public
- 2.6.11 Software malfunction
- 2.6.12 Inadequate disposal of confidential material

3. HOW TO REPORT AN INFORMATION SECURITY INCIDENT

- 3.1 All security incidents should be reported in the first instance to your immediate line manager who will ensure an incident reporting form is filled in.
- 3.2 The line manager is responsible for reporting the incident to Paul Cook, Head of Information Governance or Peter King, Head of IT.

4. SENSITIVE SECURITY INCIDENTS

- 4.1 It is recognised that some incidents can be sensitive especially if colleagues or managers may be incriminated. It is important that the person reporting the incident receives absolute protection and guarantee of confidentiality even in the event of a false alarm.
- 4.2 Sensitive incidents should be reported to an appropriate manager who will ensure that an incident reporting form is filled out and either the Head of Information Governance or Head of IT have been contacted.

5. UNINTENTIONAL BREACHES OF SECURITY

- 5.1 If an individual unintentionally causes a breach of security e.g. accidentally accessing an inappropriate web site, they should inform their line manager immediately. The reporting procedure detailed above will still be followed. If management are satisfied that the breach is accidental no disciplinary action will need to be taken.

6. SECURITY WEAKNESSES

- 6.1 Staff are required to report any observed or suspected security weaknesses e.g.
 - 6.1.1 Individuals having unlimited attempts to guess a password
 - 6.1.2 Passwords stored as readable text files which can be viewed by unauthorised individuals
 - 6.1.3 System admin privileges given to individuals who do not require them
- 6.2 Staff should not attempt to prove a suspected security weakness as this might be interpreted as a potential misuse of the system. Instead the weakness should be reported to their local IT Service Provider helpdesk and additionally

to their line manager. The line manager will ensure the weakness is reported to the Head of Information Governance, who will investigate.

7. SOFTWARE MALFUNCTIONS

- 7.1 Staff should report any instance of software malfunction to their local IT Service Provider helpdesk and additionally to their line manager, who will in turn contact Peter King, Head of IT.

Appendix 2

IM&T SECURITY POLICY

FOR

ALL EMPLOYEES AND USERS OF PCT'S IT EQUIPMENT/FACILITIES

EMPLOYEE/USER DECLARATION

The IM&T Security Policy is applicable to all permanent and temporary employees of South East Essex PCT, those people providing on-site services to the Trust under a contract and those people not employed but using the Trust IT equipment and/or facilities (e.g. remote dial-in). All employees/contractors/users must read the policy and complete the declaration below regardless of their need to access the Trust network(s).

"I _____ confirm that I have read, understood and agree to comply with the South East Essex PCT IM&T Security Policy. I understand that it is my responsibility to ensure the preservation of confidentiality, reliability and availability of data within my control and that infringement of security standards may lead to disciplinary action and/or prosecution".

By signing this declaration I also acknowledge the following.

"Any matters of a confidential nature, including particular information relating to the diagnosis of patients, individual staff records and details of contract prices and terms, must under no circumstances be divulged or passed on to any unauthorised person or persons. Any breach of such confidentiality amounts to gross misconduct warranting dismissal without notice. It is also an offence under the Data Protection Act 1998 to disclose any personal data held on computer files and can in certain circumstances result in both criminal and civil proceedings. Your attention is also drawn to the IM&T Security Policy and those System Security Policies as this may apply to you, it is your responsibility to ensure you are familiar with these documents and conform to their requirements."

Base: _____

Department: _____

Job Title: _____

Signed: _____

Date: _____

A signed copy of this declaration should be forwarded to the **IT Department**.

Suffolk House
102/108 Baxter Avenue
Southend on Sea
Essex
SS2 6JP

Tel: 01702 313700
Fax: 01702 313699