

**Mater Misericordiae Hospital**

Information Technology & Communication Usage Policy



# Information Technology & Communication Usage Policy

Policy No: 85

## Table of Contents

<b>Preface</b>	<b>3</b>
<b>Statement of Policy</b>	<b>3</b>
Information Technology and Communication Usage Policy Document	3
<b>General Principles and Policy Summary in regard to the use of IT within MMH</b>	<b>4</b>
1.0 Roles and Responsibilities	5
2.0 Terminology	6
3.0 Computing and Network Facilities	7
4.0 Information Access Environments	10
5.0 Strategic Systems	11
6.0 Data Backup Procedures	13
7.0 Communications	15
8.0 Hardware and Software Acquisition	17
9.0 Mobile Computing	19
10.0 Acceptable Use Policy for Email Usage	21
11.0 Email Request Form	23
12.0 Acceptable Use Policy for Internet Access	24
13.0 Internet Access Request Form	26
14.0 Penalties of Internet and Email Misuse	27
15.0 Web Publishing Guidelines	28
16.0 Web Author Agreement Form	38
17.0 Web Page Approval Submission Form	39
<b>Appendixes</b>	
A Backup Log Example	40
B Hardware Requisition Form	41
C Software Requisition Form	42
D HIS Account Request Form	43
E Acceptance of Responsibility Form	44
F Glossary	45

## **Preface**

### **Statement of Policy**

The identification of information as a fundamental resource in the delivery of optimum healthcare has led to the definition of the Hospital Information Technology Programme. The objective of the Information Technology Programme is to provide a secure information systems environment in support of all staff in their use of information and associated computer technology consistent with their individual needs and in accordance with the objectives of the hospital's information technology programme.

### **Information Technology and Communication Usage Policy Document**

This document defines the policies and procedures to enable the hospital to provide a secure information systems environment in support of all staff in their use of information and associated computer technology, consistent with their individual needs and in accordance with the objectives of the hospital's Information Technology Programme without risking the integrity of the organisation and its most important asset, information. It draws upon various legislative frameworks, including the Data Protection Act 1988, and the Freedom of Information Act 1997. The policy also adheres to all other relevant hospital policies and procedures including the Disciplinary Policy.

This document outlines the following:

- The Elements that constitute Information Technology (IT) security
- Explains the need for IT security
- Specifies the various categories of IT
- Indicates the security responsibilities and the roles of each user
- Indicates appropriate levels of security through standards and guidelines

## **General Principles and Policy Summary in regard to the use of IT within MMH**

The Mater Misericordiae Hospital acknowledges an obligation to ensure appropriate security for all IT data, equipment, and processes in its domain of ownership and control. Every member of staff, employed by the hospital shares this obligation to varying degrees.

Mater Misericordiae Hospital computing resources are available for use by authorised individuals, which include administrators, staff and students of the hospital. Each user shall act in an ethical manner consistent with the stated goals and IT mission of Mater Misericordiae Hospital. Each user is responsible for their use of computing resources. The hospital has the responsibility to provide appropriate security, to maintain reliability and data integrity, and to enforce this policy.

Information Technology Policy statement:

1. Users shall not under any circumstance misrepresent their identity, role or affiliation in the use of MMH IT resources.
2. All equipment and information in the hospital environment is to be used for authorised job functions only. All information within the MMH domain should remain within that domain, unless explicit permission has been granted to the contrary.
3. Those who use MMH electronic communications facilities are expected to do so responsibly, that is, to comply with state laws, with this and other policies and procedures of the hospital, and with normal standards of professional and personal courtesy and conduct.
4. [username@mater.ie](mailto:username@mater.ie) is the only valid email address supported and maintained by the Management Services Department
5. The MMH official Internet web-site is <http://www.mater.ie>
6. The MMH official Intranet is <http://minerva.mater.ie> The Intranet is for hospital staff only and is not available to the public.
7. All assets supported by the Management Services Department must have an asset number on it. It is the users responsibility to ensure their equipment is listed in the asset register.
8. Changing wiring, connections or placement of computing resources is prohibited. No piece of equipment should be moved from its registered location without consultation with the Management Services Department.
9. User must not install any software on MMH computers nor use unauthorised software unless prior written approval is obtained from the Management Services Officer.
10. External users (e.g. System Suppliers, other hospital etc) of the hospital's computing and network facilities must adhere to this policy with regard to the usage of the system.
11. It is the individual's responsibility to ensure that their information and data is effectively backed up. The Management Services Department (MSD) commits to providing reasonable facilities to do so, including where necessary, equipment, software and training but excluding consumables (unless the backup facilities are hosted by the MSD).
12. Access to hospital network facilities is strictly forbidden to mobile-computing employees unless the Management Services Department has first given clearance. Only designated network points shall be used for mobile-computing use.
13. Under no circumstances should any web page or file on or accessed from MMH contain any material considered obscene, vulgar or pornographic.
14. Where hospital users are concerned, it is the responsibility of each Department Head to ensure that this policy is enforced, and that guidelines are followed wherever possible.
15. The hospital, through authorised individuals, reserves the right to periodically check and monitor the computing and networking facilities and reserves any other rights necessary to protect them.
16. The MMH reserves the right to take disciplinary action, against staff members, who have contravened the Information Technology Policy.
17. The hospital reserves the right to take emergency action to safeguard the integrity and security of the computing and networking facilities. This may include the removal of services without prior warning.
18. The user is responsible for the security of their password. This includes making sure nobody else knows it. The Management Services Department will not provide any users with their current passwords, permissions or access information over the telephone.

## **1.0 Roles and Responsibilities**

### **1.1 Hospital Management**

The Hospital Computer Committee is responsible for:

- Resolving issues in regard to all matters relevant to the appropriateness of this policy
- Ensuring that standards of technology are continuously reviewed.
- Departmental heads/staff are kept informed of Computer Committee recommendations.
- Clear direction is given to department heads as to the importance of this policy and the correct adherence to it.

### **1.2 Heads of Department**

The Head of Department must ensure that:

- The Policy is understood and enforced within their department
- The Management Services Department are notified of any staff changes and/or change of employees functions
- The Computer Committee are informed of any breaches of the Policy
- All equipment and software is registered with the Management Services Department for support reasons.

### **1.3 Management Services Department**

The Management Services Department is charged with the responsibility, of implementer of the policy by the Board of the Hospital, and part of its role and function is to continuously enhance and maintain the technological infrastructure of the hospital, its facilities and equipment within the financial targets allocated. The Management Services will act on behalf of the hospital to develop, implement and support hospital policy on information and associated technology.

### **1.4 Hospital Staff**

All employees of the Hospital should:

- Inform their Department head of any breaches in the policy
- Backup their data regularly
- Keep their password secret and change it regularly to ensure no security breaches occur.

## 2.0 Terminology

The following terminology and definitions may be used throughout the Information Technology Security Policy.

### 2.1 Disciplinary Action

Mater Misericordiae Hospital may take disciplinary, against staff members, who have contravened the Information Technology Policy. Such action may take the form of oral or written reprimands by the staff members Head of Department. Where serious contraventions have taken place, the case will be taken to the Human Resources Department, who shall take appropriate action. Any action will follow the Disciplinary Procedure as outlined by the Hospital.

### 2.2 Appropriate & Responsible Use

Use that is consistent with the maintenance of the highest standards in the provision of patient care, research and educational services of the Hospital, and with the specific objectives of the project or task for which such use was authorised. *(It should be noted that all uses inconsistent with these objectives are considered to be inappropriate use)*

### 2.2 Illegal Activity or Usage

Illegal Activity or Usage may be described under a number of different headings:

- National Security
  - Terrorist activities
  - Instructions on bomb making
  - Hacking into government computer networks
- Injury to Children
  - Child pornography
  - Adult pornography
  - Material depicting extreme violence
  - Child trafficking
  - Advice on anonymous exchange of graphic material
- Injury to Human dignity
  - Racial discrimination, incitement to racial hatred
  - Extreme sexual perversion
- Economic security
  - All types of fraud
  - Instructions on credit card privacy
- Information Security
  - Malicious Hacking
- Privacy Protection
  - Unauthorised mailing
  - Interception of personal e-mail
  - Misuse of personal data
  - Unfair obtaining of personal data
- Protection of Reputation
  - Libel
- Gambling
- Information on or sale of 'controlled drugs'
- Intellectual Property
  - Copyright infringements of any medium
  - Unauthorised distribution of software, etc

### 2.4 Objectionable Material

Objectionable or harmful material is made up of that material which, while not illegal, is capable of causing harm to the individual. This harm can arise because of particular characteristics of the individual, age, sex, race, etc., or it can be linked to the nature of the material itself. The control of harmful or objectionable material that is not illegal must lie more in the domain of the individual.

### **3.0 Computing and Network Facilities**

#### **3.1 Introduction**

This document details the core conditions and codes of practice for all types of Computing and Network facilities that are available for use by staff. It is therefore of extreme importance that all staff members are aware of these issues and are familiar with the context of their own working environment within which these conditions and codes of practice apply.

#### **3.2 Conditions and use of computing & Networking facilities**

It is the policy of the Hospital that its computing and networking facilities are intended for use in support of the hospital's mission. Although recognising the increasing importance of these facilities to the activities of staff, the Hospital reserves the right to limit, restrict, or extend access to them.

All persons using the computing and networking facilities shall be responsible for the appropriate use of the facilities provided as specified by the '*Codes of Practice*' of this policy.

The Hospital will endeavour to safeguard the possibility of loss of information within the Hospital's computing and networking facilities. All users have a responsibility firstly not to hinder, and secondly to assist the hospital in this endeavour. The user must take all reasonable measures to further safeguard against any loss of information within the Hospital's computing and networking facilities.

Users of the computing and networking facilities recognise that when they cease to be formally associated with the Hospital (e.g. no longer an employee), their information may be removed from Hospital computing and networking facilities without notice. Users must remove their information or make arrangements for its retention prior to leaving the Hospital.

The Hospital reserves the right to limit permanently or restrict any user's usage of the computing and networking facilities; to copy, remove, or otherwise alter any information or system that may undermine the authorised use of the computing and networking facilities; and to do so with or without notice to the user in order to protect the integrity of the computing and networking facilities against unauthorised or improper use, and to protect authorised users from the effects of unauthorised or improper usage.

The Hospital, through authorised individuals, reserves the right to periodically check and monitor the computing and networking facilities, and reserves any other rights necessary to protect them.

The Hospital reserves the right to take emergency action to safeguard the integrity and security of the computing and networking facilities. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords.

Disciplinary action will be taken if staff members have been found to be: -

- Responsible for wilful physical damage to any of the computing and networking facilities;
- In possession of confidential information obtained improperly;
- Dissemination of information without appropriate permissions.
- Responsible for wilful destruction of information;
- Responsible for deliberate interruption of normal services provided by the Management Services Department;
- Gaining or attempting to gain unauthorised access to accounts and passwords;
- Gaining or attempting to gain access to restricted areas without the permission of the Management Services Department staff;
- Responsible for inappropriate use of the facilities.

External work or any use of the computing and networking facilities shall not be undertaken which would hinder or prevent Hospital users from having their usual access to the facilities.

External users (e.g. System Suppliers, Community Health Practitioners, Other Hospitals) of the Hospital's computing and networking facilities must adhere to this policy with regard to usage of the system.

### **3.3 Code of Practice**

The purpose of the Code of Practice is to specify user responsibilities and to promote the appropriate use of IT for the protection of all members of the Hospital community. Users of the Mater Misericordiae Hospital computing and networking facilities accept the following specific responsibilities:

- To safeguard their data, personal information, passwords and authorisation codes, and confidential data;
- To take full advantage of security mechanisms built into the computing systems and to follow the security policies and procedures established to control access to and use of administrative data.
- To respect the privacy of other users; for example, not to intentionally seek information on, obtain copies of, or modify files, tapes, or passwords belonging to other users or the Hospital;
- Not to represent others, unless authorised to do so explicitly by those users;
- Not to divulge any personal data to which they have access concerning staff or patients without explicit authorisation to do so.
- To respect the rights of other users; for example, to comply with all Hospital policies regarding religious, sexual, racial, and other forms of harassment.
- To respect the legal protection provided by copyright and licensing of programs and data; for example, not to make copies of licensed computer programs.
- To respect the intended usage of systems for electronic exchange (such as e-mail, Usenet News, World Wide Web, etc.) that is to improve patient care and the ease of communication on work related matters. The system is not to be used to send forged electronic mail, mail that will intimidate or harass other users, chain messages that can interfere with the efficiency of the system, or promotional mail for profit-making purposes. Also, not to break into another user's electronic mailbox or read someone else's electronic mail without their permission.
- To adhere to all general Hospital policies and procedures including, but not limited to, policies on proper use of information resources and computing and networking facilities; the acquisition, use, and disposal of Hospital-owned computer equipment; use of telecommunications equipment; legal use of software; and legal use of data.
- To report any information concerning instances in which the Hospital IT Policy or any of its standards and codes of practice has been or is being violated.

### **3.4 Code of Practice for specific Activities**

The following apply to specific activities:

#### **3.4.1 Illegal Activity**

In general, it is inappropriate use to store and/or give access to Information on the Hospital computing and networking facilities that could result in legal action against the Hospital unless strictly permitted under the Freedom of Information and the Data Protection Act.

#### 3.4.2 Objectionable material

The Hospital's computing and networking facilities must not be used for the transmission, obtaining possession, demonstration, and advertisement or requesting the transmission of objectionable material.

#### 3.4.3 Harassment

Hospital policy prohibits sexual and discriminatory harassment. The Hospital's computing and networking facilities are not to be used to libel, slander, or harass any other person. The following constitute examples of Computer Harassment:

- Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family;
- Intentionally using the computer to disrupt or damage the care giving, academic, research, administrative, or related activities of another;
- Intentionally using the computer to invade the privacy of another or the threatened invasion of the privacy of another.
- The display of offensive material in any publicly accessible area is likely to violate Hospital harassment policy. There are materials available on the Internet and elsewhere that members of the Hospital community will find offensive. The Hospital cannot restrict the availability of such material, but it considers its display in a publicly accessible area to be inappropriate. Public display includes, but is not limited to, publicly accessible computer screens and printers.

#### 3.4.4 Wasting Resources

It is inappropriate use to deliberately perform any act, which will impair the operation of any part of the computing and networking facilities or deny access by legitimate users to any part of them. This includes but is not limited to wasting resources, tampering with components or reducing the operational readiness of the facilities.

The wilful wasting of computing and networking facilities resources is inappropriate use. Wastefulness includes but is not limited to passing chain letters, wilful generation of large volumes of unnecessary printed output or disk space, wilful creation of unnecessary multiple jobs or processes, or wilful creation of heavy network traffic. In particular, the practice of wilfully using the Hospital's computing and networking facilities for the establishment of unnecessary chains of communication connections is an inappropriate waste of resources.

#### 3.4.5 Game Playing

Hospital computing and network services are not to be used for game playing. Game playing is not permitted unless it is part of an authorized and assigned research or instructional activity. Extensive or competitive recreational game playing is prohibited.

#### 3.4.6 Commercial Use

Hospital computing and network facilities are provided by the Hospital for the support of its mission. It is inappropriate to use the computing and networking facilities for:

- Commercial gain or placing a third party in a position of commercial advantage
- Any non-hospital related activity, including non-hospital related communications.
- Commercial advertising or sponsorship except where such advertising or sponsorship is clearly related to or supports the mission of the Hospital or the service being provided.

#### 3.4.7 Use for Personal Business

Hospital computing and network facilities may not be used in connection with compensated outside work or for the benefit of organisations not related to the Mater Misericordiae Hospital.

## **4.0 Information Access Environments**

### **4.1 Introduction**

This section outlines the policy of the Mater Misericordiae Hospital with regard to the Information Access Environment that is made available to users to enable them to carry out work related activities.

### **4.2 The Mater Desktop Environment**

While underlying technologies may change (e.g. Windows 95 to Windows 98), the requirement of users for simple, fast, and reliable access paths to systems and applications does not. With the implementation of a standard desktop environment for all levels of Hospital personnel, this will allow Management Services personnel to react quickly and efficiently to resolve issues that come in the way of this access mechanism.

The Mater Desktop Environment ensures:

- Similar look and feel for all users.
- Ease of access to systems and applications both on the local machine and on remote systems.
- Ease of maintenance for Management Services Staff.

### **4.3 Desktop Environment Maintenance**

To ensure that the Desktop is usable by all designated staff, the following guidelines must be adhered to:

- Users must not attempt to change, alter or delete any of the settings that exist on the Desktop. This includes Network settings, Control Panel settings, and Icons that exist on the Desktop itself.
- If a screen saver password is used, then all staff that will be using the computer must be informed.
- Users should perform orderly shutdowns of their computer. This will ensure that problems associated with improper shutdown are minimised.

### **4.4 Virus Protection**

- Virus Scanning Software: Hospital approved software shall be installed. The user must ensure that this software is updated on a regular basis for new viruses and variants.

## **5.0 Strategic Systems**

### **5.1 Introduction**

This document outlines the procedures that are carried out by the Management Services Department in regard to the day-to-day running of strategic systems.

### **5.2 Management of Strategic Systems**

A strategic system is one that meets several of the following criteria specified in the Mater Misericordiae Hospital IT Strategy.

- Critical to the mission of the Hospital
- Affects large parts of the Hospital
- Yields hospital-wide benefits

Strategic platforms and Applications are managed and operated by the Management Services Department in conjunction with System Suppliers, with the exception of the Pathology System where control of access is managed by the Pathology Department. The following Strategic Systems are considered and mentioned in the context of this document and other documents that refer to 'Strategic Systems'

- Patient Administration / Hospital Information Systems (including Financial Systems)
- Laboratory System
- Medical Imaging System (including Radiology Management System)
- Networking
- Internet / Intranet / Email Systems

### **5.3 User Access**

#### 5.3.1 New Users

The allocation of Usernames and Passwords for all systems shall be carried out in the following manner. All prospective and existing users of such systems should note that an Acceptable Usage Policy, which all users must abide by, governs the use of all such systems.

- Application for access to any of the strategic systems must be made to staff of the Management Services Department.
- In the case of the Hospital system, the applicant must present themselves to the Management Services Department or be met by Management Services personnel in the main hospital. The applicant must present suitable personal identification. Also, the user must bring with them a form (sample included in Appendix D) outlining, what function set they require, duration of access and this must be signed by department head or staff supervisor for relevant section. A list of all function sets can be obtained from the Management Services Department if required.
- The applicant shall fill out the relevant required detail as well as giving a signature and date. The Management Services Staff member then retains this. For some systems, it will be possible for a username and password to be given to the user at this point. For all other cases, Management Services shall convey this detail in writing or in person.
- The signed card will be kept indefinitely by the Management Services Department or until notified by the Human Resources Dept that the individual is no longer employed by the hospital.
- The level of access will be no higher than required as approved by the Management Services Department.

#### 5.3.2 Terminating Users

The Human Resources Department will give notification of staff leaving the hospital and those accounts must be disabled or removed from all systems. With email, accounts shall be

disabled and aliases to the new address can be set up for a short period (usually 4 weeks). With network accounts where data is held, access to the data will be granted to the department head, whose responsibility it is to distribute it to other relevant members of staff.

Passwords and codes, which are being used by staff members to gain access to systems, or to buildings or rooms where computer associated hardware and networking equipment is situated, will also be changed.

### 5.3.3 Password Aging

Password aging will be carried out for strategic systems as decided by the Operations Manager. The Operations Manager shall inform relevant Management Services Staff when this occurs.

## **5.4 Data Integrity**

Security backups of all data will be made daily. The backup regime must meet the following criteria:

- Enable recovery to at least the start of business on any weekday of a failure.
- Provide at least one more level of backup to a previous time, to cover the case of the failure of the primary backup media.
- There must be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.
- There must be a validation of security backup media at least once every six months.

## **5.5 Physical Security**

The following standards of physical security of strategic platforms must be met:

- Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.
- Air temperature and humidity must be controlled to within acceptable limits.
- Platforms must be electrically powered via UPS to provide the following:
  - o Minimum of 15 minutes' operation in the event of a power blackout.
  - o Adequate protection from surges and sags.

## **5.6 Physical Access**

- Premises will be staffed and controlled by designated Management Services Department Staff.
- External doors will remain locked.
- The premises will be fitted with suitable alarm facilities.
- In the event of alarm, either HCC or Security personnel shall contact the On-Call person.

## **5.7 Fire Detection and Control**

- There will be smoke and thermal detectors on the premises.
- Under floor areas will have smoke and water detectors.

## **5.8 Documentation**

Technical, Operations and End User Documentation will be available for Management Services Department staff in appropriate and agreed areas. All documentation will be available via a web server. It is the responsibility of individuals to ensure that they have printouts of the most recent versions of these electronic documents.

## 6.0 Data Backup Procedures

### 6.1 Introduction

This document outlines the responsibilities of all members of staff with regard to Data Backup Procedures. Those who do not adhere to these guidelines risk the possibility of losing information, which may be impossible to retrieve.

***Please note that it is the individual's responsibility to ensure that their information and data is effectively backed up. The Management Services Department shall not be held responsible for any loss of data or information on these computers.*** All staff computers will be maintained to the level recommended in this document both with regard to hardware and software, which is supported by the Management Services Department.

### 6.2 File Naming Conventions

Where possible, file names should indicate the content of the data contained within it. This is especially the case where many users may be sharing a file.

#### 6.2.1 Directory/Folder Naming Conventions

Information and data can be categorised in the Mater Hospital into seven main categories. They are Word Processing, Spreadsheets, Presentations, Databases, Multimedia, Statistical Analysis and Online Data retrieval.

As a guideline all data and information files from the applications mentioned above should be held in a directory called \Data. All of the directories mentioned below are sub directories of this. Theoretically, this data may be contained on hard disk (C, D etc) or floppy, lomega zip, or other storage media.

- *Word Processing:* All word processing documents should be contained within the directory \docs
- *Spreadsheets:* All spreadsheets should be contained with the directory \ssheets.
- *Presentations:* All presentations should be held within the directory \present.
- *Databases:* The management services department would normally provide these, and so guidelines would already be in place for where this data is actually stored. Where database applications are obtained from other than the Management Services Department, then the users should be aware of the backup procedures and recommendations that the supplier advises. Where multi-user access is required for these databases, and then the data will either be located on a shared area of the user's computer or an area of the server.
- *Multimedia:* In this context we mainly refer to text and images (e.g. telemedicine applications). Files of these types should be held within the directory \Mmedia and have appropriate sub directories for different applications (e.g. \Telepathology or \Images). Valid file extensions, which may be held within this directory, will include jpg, bmp, tiff, avi, wav, au.
- *Statistical Analysis:* Files of these types should be held within the directory \Stats.
- *Online Data Retrieval:* This would include software and data associated with laboratory analysers, assay machines, dialysis equipment etc. These would normally have a dedicated computer, which is linked either directly or indirectly via the network.

#### 6.2.2 Application Directories and Folders

When Management Services Personnel or other staff is installing applications then the following conventions should be adhered to:

- All default directory locations for applications should be used when no alternative drive is available.
- Where default directory locations for applications are not given, then the installer should choose the most obvious directory name. If this application is to be installed on a number

of computers within the hospital then this directory name should be used as a standard on all other installations.

### **6.3 Backup Procedures**

#### 6.3.1 Storage Media

The most common storage media associated with the large-scale backup of computer data are magnetic disks and magnetic tapes. These can include:

- Floppy disk
- Hard disk
- Network Drives or Disks
- Iomega Zip & Jaz

#### 6.3.2 User Backup Procedures

- All backups or replication of data to other media should be carried out whenever there are significant changes to a file or number of files. It is recommended that this be carried out at least once a day, preferably at lunchtime or just after finishing for the day. Where several users are using the one computer, then it should be responsibility of one person to actively backup information that is used by the group. Where one person uses an application on a computer that is by other personnel for other task, then it is the responsibility of this individual to backup the data for this application.
- All media should be labelled and dated with the data it contains.
- All magnetic media including floppy diskettes and Iomega Zip drives should be stored according to the instructions and guidelines suggested by the manufacturer.
- All magnetic media should be stored in a safe secure place.
- Where a user is having problems with recovering a file from any type of magnetic media type, then all data, where possible should be recovered, written to another media, and the original destroyed.
- A backup log should be maintained. This log should record the date/time, tape number, backup operator's name. Log enables users to retrieve data more quickly if they know when the last good backup was taken. A sample backlog is included in Appendix B for user reference.

## **7.0 Communications**

### **7.1 Introduction**

This document outlines the policy of the Mater Misericordiae Hospital with regard to the Communications Infrastructure, which provides access of its strategic systems to Software Suppliers, Communication Vendors, Healthcare Institutions, and external users of Mater Hospital Systems. This document also details the obligations of users and the methods of access that are used to communicate with both strategic and external systems and the impact the geographical location of such a user will have on access to these systems.

### **7.2 Network Geography**

The Mater Hospital Network that exists behind the Hospital Firewall is composed of three major LANs – Public, Private and Partner. Access from one network to another is not possible without direct configuration being carried out by the Network Controller.

#### 7.2.1 Public Network

The Mater Hospital Public Network is that network which is fully visible to the outside world. Primarily, this network contains web servers, which maintain the Hospital's presence on the Internet.

#### 7.2.2 Private Network

The Mater Hospital Private Network is that network on which all strategic systems operate. This network is physically separate from other parts of the Hospital Network.

#### 7.2.3 Partner Network

The Mater Hospital Partner Network is that network, which is not visible to the outside world, but is accessible to those people or organisations that require access to strategic systems on the Private Network.

### **7.3 Access to the Partner Network**

#### 7.3.1 Access Types

Access to the Partner Network shall be considered and reviewed for existing and prospective external users and suppliers of Strategic Systems by the Management Services Officer in conjunction with the Network Controller.

Each request for access shall be considered in isolation from other such requests. Where a request is turned down, it is the position of the Management Services Department that it is not obliged to inform the applicant of the reason for refusal of service. This information the Management Services Department deems could possibly lead to a compromise of the Hospital Network.

The conditions of use for such access to be obtained contain a generic set of requirements.

- Services to be accessed must run on the TCP/IP Protocol
- Encryption software shall be used to ensure that services that are accessed over the public Internet shall be secure and confidential.

Once agreement has been reached on the points mentioned above, the process can move on to the next step. These requirements may vary depending on the role of the applicant (e.g. Software Supplier, Healthcare Institution, Hospital Employee) and the method of access (e.g. via the Internet, Leased Line, ISDN, PSTN etc.).

#### 7.3.1.1 Software Supplier, Other Healthcare Institution

Before any further discussion takes place, each party shall informally discuss and formally exchange documentation relating broadly to Security Policy but with specific regard to communication between it and external entities. The Mater Hospital reserves the right to discontinue discussion if access to these documents is disallowed. Where an organisation has only an informal Security Policy, then the Mater Hospital shall reserve the right to discontinue discussion. It is the wish of the Mater Hospital that where a formal Security Policy exists, then this Policy be recognised as Official Organisational Policy by the Chief Executive,

Chairperson, President or Managing Director of the Organisation. If this is not the case, then the Mater Hospital shall reserve the right to discontinue discussion.

Where agreement has been reached on the content of the Mater and third party security policies, further technical detail may be required from both organisations. This will include discussion of links that each party has with other organisations and the possible implications of such links. Formal documentation reviewed at this stage shall include Network Topography diagrams.

A confidentiality clause shall exist between the parties involved. This shall be in the form of a standard clause between the Hospital and any party, which has access to confidential patient clinical and administrative information as a result of work that it carries out on behalf of the Hospital.

#### 7.3.1.2 Hospital Employee Off-Site

Certain Hospital employees may be given access to some of the Hospital Strategic Systems from other locations (e.g. Home, Private Consultation Rooms, etc). This could include Management Services On-Call Personnel, Consultants On-Call etc.

When access to the applicant has been approved, then the applicant must have the necessary encryption software installed on the source machine.

#### 7.3.2 Access Method

Access to the support network may be via the Internet, Leased Line, ISDN or PSTN.

##### 7.3.2.1 Internal User Access to External Systems

It is the policy of the Mater Hospital that all access to external systems by users from the Mater Hospital Campus be via the communications medium provided, i.e. through the Firewall. Access to any external systems via modem, ISDN connection or other means is strictly prohibited. Such access could expose the Mater Hospital Computer Network to attack.

## **8.0 Hardware & Software Acquisition**

### **8.1 Introduction**

This document outlines the responsibilities of all members of staff with regard to the acquisition of hardware and software and lays particular emphasis on the software which may be legally used by any hospital staff in the carrying out of their duties as outlined by their Mater Misericordiae Hospital Contract of Employment.

### **8.2 Restricted Software and Hardware**

Users should not knowingly possess, give to another person, install on any of the computing and networking facilities, or run, programs or other Information which could result in the violation of any Hospital policy or the violation of any applicable license or contract. This is directed towards but not limited to software known as viruses, Trojan horses, worms, password breakers, and packet observers.

The unauthorized physical connection of monitoring devices to the computing and networking facilities which could result in the violation of Hospital policy or applicable licenses or contracts is inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and networking facilities for the purpose of monitoring data, packets, signals or other information. Authorization to possess and use such hardware for legitimate diagnostic purposes must be obtained from the Network Controller of the Management Services Department.

### **8.3 Copying and Copyrights**

Users should be aware of and abide by the Hospital Policy on Copying and Using Computer Software. Most software that resides on the computing and networking facilities is owned by the Hospital or third parties, and is protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses.

### **8.4 Requisition of New Hardware**

To ensure that a consistent level of service is provided by the Management Services Department with regard to the maintenance and upkeep of hardware devices and equipment, it is imperative that the following guidelines be maintained with regard to the purchase or acquisition of these items regardless of whether the items are being purchased directly by the Management Services Department or through other means. It should be noted that the requisition of such items is dependent on factors such budgetary constraints. The following procedures shall be carried out when it is identified that new hardware is required:

- The requesting department should identify the purpose of the new equipment and whom it will be used by.
- The requestor should fill out the [Form for Requisition of New Hardware](#) (see Appendix B) in conjunction with the head of the Department. This form details the current hardware items, which the Management Services Department may routinely purchase for Hospital Departments. The letter should be addressed to the Management Services Officer. It is important that the use of the hardware is outlined as the Management Services Department may be in a position to offer an alternative solution to the one initially proposed.
- On receipt of the hardware items, it is the prerogative of the Management Services Department as to whether the hardware and associated configuration occurs in the requestor department, in the Management Services Department or at a specialist installation site outside the confines of the hospital. Where an off-site installation is involved, the requesting department should inform the Management Services Department of the existence of sensitive information contained on any hardware equipment. It is the responsibility of the Requestor Department to ensure that this

information is removed or otherwise protected while the equipment is not within the confines of the department.

The Management Services Department reserves the right to not to proceed with the purchase and requisition of a particular item of hardware where an accompanying letter is not received from the Head of the requesting Department.

Where hardware items are not being purchased through the Management Services Department, it is imperative that the Department in question liaise closely with Management Services to ensure that the equipment purchased is considered compatible with the rest of the Hospital's currently supported computer equipment. Where an incompatibility exists, or where this liaison has not occurred then the Management Services Department reserves the right to review the support services that it provides to a particular department on the basis that it may not be able to carry out this role given the issues which may arise with the support of this hardware in the future.

### **8.5 Requisition of New Software**

The Management Services Department is responsible for the provision of Application Software packages to all users throughout the hospital - Application Software includes Word Processing, Spreadsheet, Desktop Databases and Presentation Software. The Management Service Department is also responsible for the upkeep and maintenance of all Licensing issues surrounding the use of this software.

Where new software is required to be installed on Hardware owned by the Hospital the following procedures shall be adhered to:

- The requesting department should identify the purpose and need of the new software and who will use it.
- The requestor should fill out the [Form for Requisition of New Software](#) (see Appendix C) in conjunction with the head of the Department. This form details the software applications, which are currently supported by the Management Services Department. This letter should be addressed to the Management Services Officer.
- On receipt of this letter, the Management Services Officer may liaise with his staff to obtain more detailed information with regard to this request. The operating conditions of the software (e.g. to ascertain if the destination hardware shall be capable of running the application) will be evaluated.
- If the evaluation of the operating environment is not successful, then the Management Services Officer shall be made aware of this and make a decision accordingly as to whether the necessary steps (e.g. purchase of new equipment by the Management Services Department) to allow this request to be successful should continue.
- The Management Services Department reserves the right to not to proceed with the installation of particular piece of application software where an accompanying letter is not received from the Head of the requesting Department.

Where software packages are not being purchased through the Management Services Department, it is imperative that the Department in question liaise closely with Management Services to ensure that the software purchased is considered compatible with the rest of the Hospital's currently supported computer software and applications. Where an incompatibility exists, or where this liaison has not occurred then the Management Services Department reserves the right to review the support services that it provides to a particular department on the basis that it may not be able to carry out this role given the issues which may arise with the support of this software in the future.

## **9.0 Mobile Computing**

### **9.1 Introduction**

This document outlines the policy of the Mater Misericordiae Hospital with regard to the use of mobile computing equipment. The mobile-computing equipment covered by this document includes notebooks, handheld computing devices, and related peripheral devices and options, as well as all associated software. This document does not include in its brief regulations relating to the use of smaller computing devices, such as electronic address books etc.

### **9.2 Ownership**

The Mater Hospital retains all risk of loss or damage to hospital-owned mobile-computing equipment while the equipment is in an authorised employee's possession unless that damage or loss can be attributed to the employee's negligence.

The Mater Hospital retains all rights; interest and title to Mater Hospital provided mobile-computing hardware and software. Return of this equipment is required in the event of an employee's departure or upon demand by the Mater Hospital.

Mobile-computing equipment and software provided by the Mater Hospital may not be altered without the approval of the Management Services Department Support Personnel.

Mobile-computing equipment and software provided by the Mater Hospital may not be loaned or assigned to a non-employee. Loans or assignments to another Hospital employee require the approval of the Management Services Officer or Department Head. Use by an employee's family members is explicitly forbidden.

The Mater Hospital reserves the right to examine all Hospital owned mobile-computing equipment for compliance with information management policies. The Mater Hospital also reserves the right to examine employee-owned mobile-computing equipment for the unauthorised existence of hospital or patient related data.

### **9.3 Security**

Any data or information files contained on Mobile-computing equipment must be managed in keeping with the Mater Hospital Security Policies to prevent loss, disclosure, modification or destruction.

Employees have the responsibility of maintaining adequate physical protection of their Mater Hospital provided mobile-computing equipment. This includes, but is not limited to, leaving the equipment unattended in public areas or leaving the equipment in plain sight.

Dial-up-access information, including telephone numbers and user IDs, must be kept confidential by the mobile-computing employee to prevent unauthorised access to Mater Hospital host systems, if such access has been given.

A boot-up password should be implemented on the device. This password should be memorised and should not be written down to aid memory.

### **9.4 Access to Hospital Network Facilities**

Access to Hospital Network Facilities is strictly forbidden to mobile-computing employees unless the Management Services Department has first given clearance. Employees must apply in writing for dial-in access. Where employees have permission to gain access to these facilities, they must abide by the following conditions:

- Access only to be given in private areas not normally accessible to the public. Where access is to be given in clinical areas like outpatient departments, then due care must

be enforced with regard to the security of the mobile-computing device (e.g. laptop must be secured with a cable-lock kit to a desk or other fixed piece of furniture).

- Only designated network points shall be used for mobile computing use.

When access is to be given to a Hospital Networked facility through a mobile computing device then the Management Services Department will first audit the device for the following:

- Virus Scanning Software: Hospital approved software shall be installed. The user must ensure that this software is updated on a regular basis for new viruses and variants.
- Software availing of Network services: Software, which needs network services as an intrinsic part of its function, shall be audited for acceptability and conformance to Mater Hospital Software standards. This would include games and Internet related software provided by ISP's.
- Details including device serial number, MAC address of Network card, hardware and software details shall be recorded and signed as being correct by the user. This will allow tracking of Mater Hospital network and system facilities by Management Services Department staff.



Information technology resources are provided by the hospital to further the hospital's mission of patient care, education and research. Use of these resources must be consistent with this mission and this policy. Inappropriate use of email will result in an immediate cancellation of the mail account. Mater Misericordiae Hospital provided e-mail, like computer systems and networks, is considered hospital resources, and is to be used for hospital purposes only. Usage may be monitored for unusual or inappropriate activity. Any decision the Management Services Department makes in relation to its services will be final on all matters.

***Users shall not under any circumstance misrepresent their identity, role or affiliation in the use of Mater Misericordiae Hospital information technology resources.***

### **Representation**

Users of electronic communications facilities shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the hospital unless appropriately authorised (explicitly or implicitly) to do so. While it is permissible to indicate one's affiliation with the hospital, unless it is clear from the context that the author is not representing the hospital an explicit disclaimer shall be included. An appropriate disclaimer may take the form: "These statements are my own, not those of the Mater Misericordiae Hospital"

### **Email Software**

As outlined in the Software section, users of the Mater Hospital email system shall only use software approved by the Management Services Department for sending and retrieving email. The use of other non-approved software is not permitted, and Management Services Department Staff shall not support such software.

### **Electronic Mail Regulations**

The content and maintenance of a user's electronic mailbox is the user's responsibility:

1. All messages shall be purposeful and appropriate.
2. Email should be courteous and polite and be consistent with hospital policies
3. Email should protect others right to privacy.
4. Email should not contain obscene, offensive or slanderous material.
5. Check E-mail daily and remain within your allocated disk quota.
6. Delete unwanted messages immediately since they take up disk storage.
7. Keep messages remaining in your electronic mailbox to a minimum. Remember to empty your Deleted Items folder regularly.
8. Mail messages can be downloaded or extracted to files then to disks for future reference.
9. Refrain from sending or answering Chain Mail/Junk Mail as it affects the amount of traffic on the network. Use of email may be subject to monitoring for security and/or network management reasons.
10. Double-check all "To:" fields prior to sending messages
11. Avoid leaving open e-mail on the computer screen. If the computer is in the same room as other patients, use password protected screen savers so that patient files are not visible to other patients.
12. As with other parts of the medical record, patient-identifiable e-mail must not be taken out of the hospital domain.
13. Email messages can be forged in the same way as faxes and memoranda. If a message is suspect, users should verify its authenticity via telephone or fax.
14. Sensitive, confidential information should not be sent through email system unless it is encrypted.
15. Email should not contain information that is harmful to the hospital or members of the hospital community.

**Conditions of Use: Users shall not**

1. Represent personal opinions as those of the hospital
2. Breach the guidelines set out by the Data Protection Act in relation to patient confidentiality.
3. Use someone else's identity and password for access to information.
4. Subscribe to non-hospital authorised mailing lists. Mailing lists are schemes for distributing copies of the same email to many different people. It is not acceptable to subscribe anyone, other than a user on your own host, to any mailing list or similar service, unless their explicit permission has been given.
5. Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person
6. Solicit e-mails that are unrelated to hospital activities
7. Use the Internet or e-mail for any illegal purpose
8. Make or post indecent remarks, proposals, or materials
9. Waste time on non-hospital business

**Maintenance of Accounts**

1. Accounts may be used only by the authorised owners of the accounts
2. Users must notify the Computer Centre when they no longer require their email account
3. Passwords will expire every 90 days. Users must contact the Management Services Dept for passwords to be updated.
4. Accounts will be deleted if they are not used for 3 months.
5. User directories may also be subject to limitations.

Users who violate any of the guidelines set in the policy may be subject to disciplinary action including written warnings, revocation of access privileges, and employee termination. The Mater Misericordiae Hospital also retains the right to report any illegal violations to the appropriate authorities. The distribution of any information through email is subject to the scrutiny of the hospital. The hospital reserves the right to determine the suitability of this information.



Please read the Acceptable Use Policy carefully before signing the form. If you agree to comply with the policy, please return the completed form to the Computer Centre marked for the attention of the Internet Services Manager.

(Please complete all entries)

### User Details

Name (in Block Capitals)

Department

Contact Number / Bleep Number

Reasons for Application

PC Asset Number

Do you share this PC?

Signature

Date

Signature of Department Head

### For Office Use Only

Username

Password

Email Program

Version

Email address

Authorised by

Date

### Agreement

As an email user of the Mater Misericordiae Hospital, I agree to accept the guidelines and regulations outlined in the Acceptable Use Policy *for hospital email usage*.

Signature

Date



### Acceptable Use Policy for the Internet

Information technology resources are provided by the hospital to further the hospital's mission of patient care, education and research. Use of these resources must be consistent with this mission and this policy. Inappropriate use of the Internet will result in an immediate termination of access. The distribution of any information through the Internet is subject to the scrutiny of the hospital. The hospital reserves the right to determine the suitability of this information. Usage may be monitored for unusual or inappropriate activity. Any decision the Management Services Department makes in relation to its services will be final on all matters.

***Users shall not under any circumstance misrepresent their identity, role or affiliation in the use of Mater Misericordiae Hospital information technology resources.***

### Internet Software

Users of the Mater Hospital Internet system shall only use software approved by the Management Services Department for browsing the Internet. The use of other non-approved software is prohibited and Management Services Department Staff shall not support such software.

### Internet Access Regulations

1. The content of anything exchanged via Internet access (regardless of it's state of encryption) must be appropriate and consistent with hospital policy, subject to the same restrictions as any other correspondence.
2. Any person receiving disk images or programs via the Internet must conduct a virus check on them before executing or distributing them.
3. Employees granted access to many Internet connected resources need to use that access in a way which is consistent with their job function, regardless of whether the access is off-hours or on the employee's time.
4. Use of the network for recreational games is not acceptable.
5. Accounts may be used only by the authorized owners of the accounts
6. Users shall respect copyright laws and licensing agreements pertaining to material entered into and obtained via the system.
7. Any user who does not comply with the Internet Access Policy will lose network privileges. Repeated or severe infractions of the Policy may result in termination of access privileges permanently.
8. User should be aware that there is no quality control process on the Internet, and some of the data is outdated or inaccurate. Information should be checked before given to the patient.
9. The release of any Hospital Information is prohibited unless authorized by the relevant bodies.
10. In areas where the PC is in a shared area, every user that would have cause to use the PC must sign the agreement form. If users do not comply then no access will be given to that area.
11. Adult Pornography is a matter of personal choice and considered private. However, the Mater Misericordiae Hospital does not permit the hosting, transmission, re-transmission, or storage of these materials on any of hospital facilities. Offenders will have their Internet Access terminated.
12. **Child pornography is illegal.** Any user found responsible for possessing, transmitting or receiving such material will be permanently removed from the Mater Misericordiae Hospital Internet system and the appropriate law enforcement authorities notified.

**Conditions of Use: Users shall not**

1. Visit Internet sites that contain obscene, odious or other objectionable materials.
2. Breach the guidelines set out by the Data Protection Act in relation to patient confidentiality.
3. Use the Internet or e-mail for any illegal purpose
4. Represent personal opinions as those of the hospital
5. Make or post indecent remarks, proposals, or materials
6. Upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the hospital, or the hospital itself
7. Download any software or electronic files without implementing virus protection measures that have been approved by the hospital
8. Perform any other inappropriate uses identified by the network administrator
9. Waste time on non-hospital business
10. Users are not permitted to download newer version of browser software. The Management Services department must be consulted.
11. Use of the computer resources to produce or store offensive graphics or text is prohibited

Users who violate any of the guidelines set in the policy may be subject to disciplinary action including written warnings, revocation of access privileges, and employee termination. The Mater Misericordiae Hospital also retains the right to report any illegal violations to the appropriate authorities.

# Mater Misericordiae Hospital



## Internet Access Request Form

Please read the Acceptable Use Policy carefully before signing the form. If you agree to comply with the policy, please return the completed form to the Computer Centre marked for the attention of Internet Services Manager.

(Please complete all entries)

### User Details

Name (in Block Capitals)

Department

Contact Number / Bleep Number

Reasons for Application

Areas of Research

PC Asset Number

Do you share this PC?

Signature

Date

Signature of Department Head

### For Office Use Only

Computer Name

Browser & Version

Wall-box Number

IP Address

Authorised by

Date

### Agreement

As an Internet user of the Mater Misericordiae Hospital, I agree to accept the guidelines and regulations outlined in the Acceptable Use Policy for hospital Internet usage.

Signature

Date

### **13.0 Penalties for Internet and Email Misuse**

1. Stage I – Written warning. A copy of warning sent to department head and Human Resources department to be included in personnel record.
2. Stage II – Final Written Warning and or Suspension without pay. Internet/Email access will be suspended at this time.
3. Stage III – Permanent withdrawal of Internet/Email access with the possibility of disciplinary action leading to dismissal.

In the case of gross misconduct, access will be immediately terminated and dismissal procedure will be implemented.

All penalties enforced are in line with the disciplinary procedure of the hospital. Each employee when they sign their contract agrees to abide by these procedures and additionally agree to abide the Internet and Email Policies as set down by this Policy.



## Mater Misericordiae Hospital Policy on Web Publishing Guidelines

<b>Introduction</b> .....	30
<b>1. Statement of Policy in Regard to the use of Web publishing facilities</b> .....	30
<b>2. Responsibilities</b> .....	30
2.1 Hospital Management.....	31
2.2 Heads of Department .....	31
2.3 Management Services Department.....	31
2.4 Web Controllers/Editors, Web Authors.....	31
<b>3. Web Publishing</b> .....	33
3.1 Internet / Intranet Explained .....	33
3.2 Web Content Outline .....	33
3.3 Establishing a Department Web Page .....	33
3.4 Department Templates .....	34
3.5 Standards & Guidelines.....	34
<b>4. Training</b> .....	37
4.1 What to bring to Training .....	37
4.2 Training Sessions Format.....	37
4.3 Basic Training.....	37
4.4 Advanced Training .....	37
<b>Web Author Agreement Form</b> .....	38
<b>Web Page Approval Submission Form</b> .....	39

## Introduction

Over the last number of years, the Internet or World Wide Web has grown to become one of the most essential tools that can be used for communication and discourse in areas such as business, medicine, and academia and in the home. The Mater Misericordiae Hospital recognises the possibilities and benefits that exist for the use of this medium by all concerned and associated with the hospital, in whatever capacity. This includes medical, nursing, paramedical and administrative staff; general practitioners, community medicine workers; other hospitals and agencies; research and teaching colleagues from other institutions; and most importantly, the patient.

In order to ensure these facilities are utilised in the best interest of the hospital, its patients and staff an official policy in regard to the use of the Web has been defined. The successful implementation and use of the medium is reliant on a number of key strategies and guidelines, which have been adopted by the Hospital Management to support the hospital's policy.

This document defines the policy and details the strategies and guidelines:

- Statement of Policy in Regard to the use of Web publishing facilities
- Responsibilities of Hospital Management, Heads of Department and the Management Services Department
- Responsibilities of Authors of web content.
- Publishing Standards, Guidelines and Templates.
- Training
- Web Author Agreement Form
- Web Page Approval Submission Form

### 1. Statement of Policy in Regard to the use of Web publishing facilities

1. The Mater Misericordiae Hospital official web-site is <http://www.mater.ie>
2. All hospital web pages will be held on the mater web server. No page held or maintained outside the Mater domain will be published as part of the hospital web site.
3. All items published on the web site must adhere to the Hospital's Web publishing policy
4. Each page published must adhere to the official template provided.
5. Only approved graphics maybe used on the templates
6. The Web Publishing Committee is responsible for defining, interpreting and monitoring all matters relative to Web Site contents
7. Each department head is responsible for the content of their department page unless they authorise another person to do so. (See Web Page Approval Submission Form)
8. The creation, updating and monitoring of Mater Misericordiae Hospital Web pages and/or Department Web pages is restricted to employees of the Hospital. Each department head (see Web Author Agreement form) must approve web authors.

### 2. Responsibilities

The Hospital has a responsibility to its patients, staff, and the Healthcare community both at home and abroad to maintain the correct application of Web medium within the Mater Misericordiae Hospital, so as to ensure that all information, which is published, is correct, timely, informative, and up to date. The responsibility for the definition and monitoring of the hospital's web publishing standards is delegated to a hospital web editorial committee and to departmental heads in regard to departmental web publishing activities. This will result in the following allocation of responsibilities:

## **2.1 Hospital Management**

The Hospital Web Editorial Committee is responsible for:

- Resolving issues in regard to all matters relevant to the appropriateness of items to be published
- Ensuring that standards of publication are continuously reviewed.
- Departmental heads/editors/ are kept informed of Editorial Board recommendations.
- Encouragement is given to Departments to avail of Web publishing facilities.
- Personnel issues are resolved in relation to the upkeep, maintenance and continued development of Web Publishing facilities.

## **2.2 Heads of Department**

Publication of Web Content relating to a department is the prerogative of the Head of Department. The Head of Department must ensure that:

- Department Web Page is maintained in accordance with Hospital Web Policy and Guidelines
- Nominates a Web Page Controller/Editor
- Ensures the Web Page Controller/Editor attends training courses arranged by the Management Services Department and operates the Department Web Page in accordance with Hospital Web Policy and Guidelines
- Ensures the Web Page Controller/Editor is aware of recommendations that have been made by the Hospital Editorial Committee.
- Allocates appropriate resource to maintain Web Page

## **2.3 Management Services Department**

The Management Services Department maintains Web content not associated with individual departments. It also supports the infrastructure, which underpins Web Publication. This includes:

- The provision and maintenance of Web servers.
- The provision of Publishing Standards, Guidelines and Templates.
- Publishing Tools
- Training

The Management Services Department staff does not:

- Create content for any Department.
- Check Content for Publication for correctness from an Editorial standpoint.
- Take over the maintenance and upkeep of individual departmental pages that have not maintained because of resource issues within the Department.

## **2.4 Web Controllers/Editors, Web Authors**

All Web Controllers/Editors and Web Authors should:

- Ensure proposed content adheres to the Publishing Standards, Guidelines and Templates as defined in the Hospital's Web publishing policy.
- Attend training courses arranged by the Management Services Department.
- Liase with the Management Services Department to ensure that they are kept up to date of any changes to Publishing Standards, Guidelines and Templates.

- Ensure that any web content planned for publication is grammatically and syntactically correct.
- Any page containing a date must be updated/removed once that date has passed. (E.g. Information relating to a conference on the 11<sup>th</sup> July 1999, should be removed once the conference has taken place.)
- Ensure that amended content is uploaded to the ftp area on web server in before the set deadline. (This process is explained in greater detail in the training section)

### 3. Web Publishing

#### 3.1 Internet / Intranet Explained

Web Publishing in the Mater Misericordiae Hospital is facilitated for both the Internet and the Intranet. The *Internet* is the term used to describe web content that is available for access by users across the world, be they accessing the web from home, college or work. Currently, the Mater Misericordiae Hospital Internet site is hosted at <http://www.mater.ie>.

The *Intranet* on the other hand, is web content that is only made available to a specific user community, such as would be contained within a hospital or any other organisation. In the Mater Misericordiae Hospital, the Intranet is available at <http://minerva.mater.ie>

Hospital staff may access web content available on the Hospital Internet. Content on the Hospital Intranet however, *is not available for viewing outside the hospital campus.*

#### 3.2 Web Content Outline

Content location is an important consideration when creating web resources. It is important that only Hospital Staff can access information, which is pertinent to them as staff of the Hospital (*the Intranet*). Likewise, they should also be able to access information, which is available on the Hospital public Web Site (*the Internet*). From a content creation perspective, information should only be stored and maintained in one area, allowing ease of maintenance.

- Internet Content ([www.mater.ie](http://www.mater.ie)), available to the General Public
  - Hospital Facts & History
  - Patient & Visitor Information
  - Hospital Map
  - Department Information (discussed later in this document)
  - Contact Information
  - Job Vacancies
  - Newsletters (including Heart of the Mater)
  - Links to other Healthcare Institutions
- Intranet Content ([minerva.mater.ie](http://minerva.mater.ie)), available to staff only
  - Hospital Policies & Guidelines
  - Department Information (including protocols, etc)
  - Research Databases
  - Newsletters
  - Notice-boards (Social Events, For Sale, etc)

#### 3.3 Establishing a Department Web Page

Departments wishing to have a web presence should be aware of the responsibilities of all the parties necessary to ensure that such a presence can be initiated and maintained. These responsibilities, from a Department perspective necessitate that

- The Head of Department agrees the need for a Departmental Web presence
- Department Head completes Web guidelines compliance form
- Allocates appropriate resources and nominates a Department Web Controller/Editor
- Ensures all authors complete the Web Author agreement form.
- Ensures all author becomes familiar with Editorial Committee Guidelines
- Proposed Web content is within Editorial Guidelines

If a department meets all other necessary criteria outline in the Web Publishing Guidelines i.e. the provision of author and content; the Management Services Department will endeavour to provide the necessary hardware and software tools required. Provision of these tools is subject to budgetary constraints.

### 3.4 Department Templates

Templates in the web-publishing context refer to document structures that serve as a skeleton onto which content may be added. Templates contain the 'look and feel' for any content that will appear on Mater Hospital Web sites. They standardise such things as background and foreground colours, font sizes, menu appearance, etc. Individual templates within a departmental web page cater for the following:

- Introduction ([default.htm](#))
  - Profile
  - Mission Statement, Goals, Aims, Objectives
  - Expertise
  - History
- Contact Details ([contact.htm](#))
  - Address & Location
  - Phone & Fax
  - Email address
- Staff Directory ([staff.htm](#))
  - Staff names and Job-titles
  - Phone numbers
  - Email addresses
  - Bleeps (Internal use only)
- Services ([services.htm](#))
  - Inpatients
  - Outpatients (Clinic Times)
  - Consultations
  - Day Care
  - Patient Advice
- Education & Research ([research.htm](#))
  - Library Facilities
  - Research Activities
  - Publications
  - Courses, Seminars, Talks
  - Articles & Papers
  - Miscellaneous

It is mandatory that departments or units use the official templates and images provided. This provides a common "look and feel" to all Mater Web Pages and helps give the site a unique identity. Some departments may have developed web pages before this policy was in place but we ask that the authors or maintainers of such pages make their pages adhere to this policy so all pages comply. A hyperlink may be added to the official department page on the Mater web site, so as to reference this web page.

### 3.5 Standards & Guidelines

The standards included in this document are intended to promote a consistent interface for those accessing information about the Mater Misericordiae Hospital via the World Wide Web and to ensure that the quality and content of such information is in keeping with the Hospital's standards. The document is not meant to impede the creativity of Mater Misericordiae Hospital information providers nor does it address stylistic considerations or HTML authoring in detail.

- **Content**
  - The Editorial Committee must first evaluate proposed Content.
  - Standard Departmental Templates must always be used.
  - Image files must be in JPEG format and be compressed.
  - Sound files must be in .wav or .ra format.
  - Movie files must be in .mpeg or .ram format.
  - Document files must be in .doc or .pdf format or both.

- *Accuracy of Information Provided*
  - Information should be as current and accurate as possible. Inaccurate information will be reported to the information provider who is responsible for removing or revising the data. All links to Hospital and Internet resources should be checked weekly and revised as necessary.
- *Grammar and Spelling*
  - Pages should be grammatically correct without spelling errors. Acronyms should be used sparingly and never as a first reference. All web pages should employ the adopted terminology for references to the institution and its units.
- *Graphics and Fonts*
  - Graphics should provide useful, visual clues about the information provided. We recommend that your design accommodate the common screen resolution of 800 X 600 pixels. Best viewed under Netscape 3.0 / Internet Explorer 3.0 or greater.
- *Information about the author of the page/contact person*
  - Each page should include a "mail to" link at the bottom of the page for contacting the person who created or is responsible for maintaining that page.
  - Additional information such as name, title, and telephone number of the person who developed the page and/or is responsible for answering questions about the service, department, etc. should be included prominently somewhere in the set of pages (e.g. an "about" page).
  - If a generic name is given (e.g. "Cardiac Surgery," "Dialysis", etc.) the people responding to the electronic mail should have a designated person with the responsibility for answering queries. Those with the "mail to" link should respond to queries in an expedient and professional manner.
  - When the author of a web page leaves the Hospital, some other individual from the department should be assigned responsibility for answering questions related to the information on the page and for updating and maintaining the page. The page should be updated to provide an email or phone contact for the new maintainer as approved by department head.
- *Obscenity, Vulgarity and Pornography*
  - Under no circumstances shall any web page stored on or accessed from the Mater Misericordiae Hospital contain any material considered obscene, vulgar or pornographic. Neither shall any such page contain active links to such material. All pages on this site must meet the standards of decency of the Hospital and the community.
- *Publishing Mechanics*
  - Departmental image files should be contained within the /images directory.
  - Only use *absolute addressing* (e.g. <http://www.ucd.ie>) if referring to a link held on another server or site.
  - Only use *relative addressing* (e.g. /images/image.jpg) when referring to a web page or file on the current server. This *must* be maintained, as any content will first be checked on a pre-production server. If absolute addressing were used in this case, broken hyperlinks would occur.
- *Upload Of Information*
  - Contents of each department's folder, located in the FTP area of web server will be uploaded onto web site every **Friday before 9am**.
  - **Deadline** for ftp of pages will be every **Thursday at 5pm**. This time has no flexibility as backup of web server commences at 5.30pm every evening. Files ftp-ed after this time will not be included in the Friday update. Prior to FTP, the Web Page approval submission form must be completed by department head and returned to Webmaster.

- *Search Facility*
  - If you wish to be incorporated in the search facility you must adhere to the following guidelines. The Web Page approval submission form is completed accurately. It is necessary to inform the Webmaster of new pages so they can be added to the search index. If you make major changes in the content of existing pages, or remove pages/links, you should also contact the Webmaster so he can update the search index. Please note that the search engine will only index and search pages located on the [www.mater.ie](http://www.mater.ie) server.

#### 4. Training

Each web controller/editor and web authors will be provided with the following prior to attending the preliminary training sessions:

- A copy of guidelines and a Web Provider agreement form that they must sign and get co-signed by department head. The completed form must be returned to the Webmaster.
- Upon receipt of the Agreement form, web authors will have:
  - 1) The relevant authorised software installed on their machine;
  - 2) Email account set-up where necessary;
  - 3) FTP account set-up on Web Server;
  - 4) Department folder created - containing the five standard templates and official images' folder;
  - 5) Training scheduled mailed to them so that time off/cover can be arranged where applicable.

##### 4.1 What to bring to Training

Floppy disk containing information about department, which has been approved. Information is to be in Word 6.0/95 format

##### 4.2 Training Sessions Format

Training will be provided on a hands-on basis. Duration may vary (2/3 hours)

##### 4.3 Basic Training

Session 1      1) Web authors will be taught how to use FrontPage  
                    2) Create their own department pages using templates and images provided

Session 2      1) Authors will be shown how to use FTP explorer and how to upload information into ftp area of web server.

Session 3      1) Q&A format  
                    2) Comments and suggestions

##### 4.4 Advanced Training

Not every department will have an interest or need for this session. However, the course will be provided if the demand is there



## Web Author Agreement Form

---

**Completing this form will, upon approval, make you the Web Page Controller/Editor for your department** (department, division, or other group). This will mean that you will be responsible for all web-related activities for your department. The Department Head must sign this form. It should be submitted to the Management Services Department who will create an account on the web server and contact you regarding the use of that account.

### Proposed Web Controller/Editor

(Please complete all entries)

Name

Email address

Phone Number

Department/Group

PC Asset No.

---

### Department Head

Name of department head

Email address of department head

---

### Agreement

As an information provider for the Mater Misericordiae Hospital, I agree to accept the responsibilities outlined in the Web Publishing Policy *for hospital web pages* for the department designated above.

Signature

Date



## Web Page Approval Submission Form

Fill out and submit this form when you have developed a new page, debugged and tested it. To ftp onto the web server (you must be an authorised department web co-ordinator to put pages on the web server), and checked it there to make sure all features, links and graphics work. You should also have checked the accuracy of your pages. If the department head approves the page(s) for publication, they will notify the Webmaster who will upload the files on the following Friday.

### Information on content provider

(Please complete all entries)

Name

Email address

Phone Number

Department

### Where is your page?

(Please provide name of folder in FTP area)

Page is on the Web Server at the URL

### Links from other Mater Hospital pages

Specify existing pages that should have links to this new page

<input type="text"/>
<input type="text"/>
<input type="text"/>

### Department Head

(Please fill in completely and accurately)

Name of Department Head

Email address of Department Head

Signature of Department Head

Date



**Appendix B – Hardware Requisition Form**

**Management Services Officer,  
Mater Misericordiae Hospital,  
58 Eccles St,  
Dublin 7.**

**Date:**

FAO: Management Services Officer,

I would like to requisition the following hardware items from use in my department.

---

---

---

---

*Please specify use of equipment and main user(s):*

---

---

---

---

Yours sincerely

---

Head of Department

**Appendix C – Software Requisition Form**

**Management Services Officer,  
Mater Misericordiae Hospital,  
58 Eccles St,  
Dublin 7.**

**Date:**

FAO: Management Services Officer,

I would like to requisition the following software items from use in my department.

**Applications**

- |                                                           |                                           |
|-----------------------------------------------------------|-------------------------------------------|
| <input type="checkbox"/> Hospital System Access (Keaterm) | <input type="checkbox"/> Medline/Cinahl   |
| <input type="checkbox"/> Microsoft Word                   | <input type="checkbox"/> Web Browsing S/W |
| <input type="checkbox"/> Microsoft Excel                  | <input type="checkbox"/> Email Software   |
| <input type="checkbox"/> Microsoft Access                 | <b>Other Applications</b> (specify)       |
| <input type="checkbox"/> Microsoft Powerpoint             | _____                                     |

*Please detail any additional specification of software if not mentioned above:*

---

---

---

*Please specify use of software and main user(s):*

---

---

---

---

Yours sincerely

\_\_\_\_\_  
Head of Department

**Appendix D – HIS Account Request Form**

**Management Services Officer,  
Mater Misericordiae Hospital,  
58 Eccles St,  
Dublin 7.**

**Date:**

FAO: Management Services Officer,

I would like to request that a Hospital System Account would be set-up for the user(s) named below.

<u>Name</u>	<u>Function Set</u>	<u>Duration of Employment</u>
-------------	---------------------	-------------------------------

Yours sincerely

---

Head of Department

**Appendix E – Acceptance of Responsibility Form**



Please read the Information Technology Policy carefully before signing the form. If you agree to comply with the policy, please return the completed form to the Computer Centre marked for the attention of Helpdesk Administrator.

(Please complete all entries)

**Asset Details**

Asset Number <input type="text"/>	PC Make/ Model <input type="text"/>
Operating System <input type="text"/>	Wall-box Number <input type="text"/>
Authorized User(s) of PC <input type="text"/>	

**For Office Use Only**

Computer Name <input type="text"/>	IP Address <input type="text"/>
Hardware Properties <input type="text"/>	
Software Installed on PC <input type="text"/>	

**Agreement**

As a PC user of the Mater Misericordiae Hospital, I agree to accept responsibility for the above PC. I will ensure no unauthorized software is installed on this PC. I will inform the Management Services Department of any violations of the Information Technology Policy in relation to this asset. I agree to accept all the guidelines and regulations outlined in the Information Technology Policy

Signature of Department Head <input type="text"/>	Date <input type="text"/>
------------------------------------------------------	------------------------------

## Appendix F – Glossary

### A

#### **ActiveX**

A loosely defined set of technologies developed by Microsoft ActiveX is an outgrowth of two other Microsoft technologies called *OLE (Object Linking and Embedding)* and *COM (Component Object Model)*. As a moniker, *ActiveX* can be very confusing because it applies to a whole set of COM-based technologies. Most people, however, think only of ActiveX controls, which represent a specific way of implementing ActiveX technologies.

#### **Anti-Virus Program**

A utility that searches a hard disk for viruses and removes any that are found. Also known as virus scanning software.

#### **Application**

A program or group of programs designed for end users.

#### **Attachment**

A file attached to an e-mail message.

#### **Authentication**

The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from *authorization*, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

#### **Authorization**

The process of granting or denying access to a network resource and at what level (read only, create, delete and modify). Most computer security systems are based on a two-step process. The first stage is *authentication*, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.

### B

#### **Backup**

To copy files to a second medium (a disk or tape) as a precaution in case the first medium fails. One of the cardinal rules in using computers is ***back up your files regularly***. The term *backup* usually refers to a disk or tape that contains a copy of data.

#### **Biometrics**

Generally is, the study of measurable biological characteristics. In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints or speech.

#### **Browser**

Short for *Web browser*, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer.

## C

### **Cable Modem**

A cable modem is a device that enables you to hook up your PC to a local cable TV line and receive data.

### **Cache**

A cache (pronounced CASH) is a place to store something more or less temporarily. Web pages you request are stored in your browser's cache directory on your hard disk. That way, when you return to a page you've recently looked at, the browser can get it from the cache rather than the original server, saving you time and the network the burden of some additional traffic. You can usually vary the size of your cache, depending on your particular browser.

### **Case sensitive**

Being Case Sensitive means, e.g. that an attempt to open a file XXX will not match an existing file xxx in a File System.

### **Confidentiality**

A security principle that keeps information from being disclosed to anyone not authorized to access it; synonymous with secrecy.

### **Cookie**

A cookie is information that a Web site puts on your hard disk so that it can remember something about you at a later time. (More technically, it is information for future use that is stored by the server on the client side of a client/server communication.) Typically, a cookie records your preferences when using a particular site. Using the Web's Hypertext Transfer Protocol (Hypertext Transfer Protocol), each request for a Web page is independent of all other requests. For this reason, the Web page server has no memory of what pages it has sent to a user previously or anything about your previous visits. A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. You can view the cookies that have been stored on your hard disk (although the content stored in each cookie may not make much sense to you). The location of the cookies depends on the browser. Internet Explorer stores each cookie as a separate file under a Windows subdirectory. Netscape stores all cookies in a single cookies.txt file. Opera stores them in a single cookies.dat file.

### **Cryptography**

The study of encryption and decryption. From the Greek "kryptos" meaning "hidden" and "graphia" meaning "writing."

## D

### **Data**

Distinct pieces of information usually formatted in a special way. All software is divided into two general categories: *data* and *programs*. Programs are collections of instructions for manipulating data.

### **Desktop**

In graphical user interfaces, a *desktop* is the metaphor used to portray file systems. Such a desktop consists of pictures, called *icons*, which show cabinets, files, folders, and various types of documents (that is, letters, reports, pictures).

### **Directory**

A special kind of file used to organize other files into a hierarchical structure. Directories contain bookkeeping information about files that are, figuratively speaking, beneath them. You can think of a directory as a folder or cabinet that contains files

and perhaps other folders. In fact, many graphical user interfaces use the term *folder* instead of *directory*.

### **Domain**

A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains are defined by the *IP address*. All devices sharing a common part of the IP address are said to be in the same domain.

### **Domain Name**

A name that identifies one or more *IP addresses*. For example, the domain name *mater.ie* represents about a dozen IP addresses. Domain names are used in URLs to identify particular Web pages. For example, in the URL <http://www.mater.ie/index.html> the domain name is *mater.ie*

### **Download**

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network. The opposite of download is *upload*, which means to copy a file from your own computer to another computer.

### **Dial-up Access**

Refers to connecting a device to a network via a modem and a public telephone network. Dial-up access is really just like a phone connection, except that the parties at the two ends are computer devices rather than people.

### **Digital Certificate**

An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a *Certificate Authority (CA)*. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

### **Digital Signature**

An authentication tool that verifies the origin of a message and the identity of the sender and receiver. Can be used to resolve any authentication issues between the sender and receiver. A digital signature is unique for every transaction. A digital signature (not to be confused with a digital certificate) is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged. Additional benefits to the use of a digital signature are that it is easily transportable, cannot be easily repudiated, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encryption or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

### **DNS**

Short for *Domain Name System* (or *Service*), an Internet service that translates *domain names* into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every

time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.example.com* might translate to *198.105.232.4*.

## E

### Email

Short for *electronic mail*, the transmission of messages over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk. Sent messages are stored in electronic mailboxes until the recipient fetches them. To see if you have any mail, you may have to check your electronic mailbox periodically, although many systems alert you when mail is received. After reading your mail, you can store it in a text file, forward it to other users, or delete it. Copies of memos can be printed out on a printer if you want a paper copy. Another common spelling for e-mail is *email*.

### Email address

A name that identifies an electronic post office box on a network where e-mail can be sent. Different types of networks have different formats for e-mail addresses. On the Internet, all e-mail addresses have the form:

- <name>@<domain name >

For example,

- webmaster@mater.ie

Every user on the Internet has a unique e-mail address.

### Encryption

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text*; encrypted data is referred to as *cipher text*.

### Extranet

A new buzzword that refers to an intranet that is partially accessible to authorized outsiders. Whereas an intranet resides behind a firewall and is accessible only to people who are members of the same company or organization, an extranet provides various levels of accessibility to outsiders. You can access an extranet only if you have a valid username and password, and your identity determines which parts of the extranet you can view. Extranets are becoming a very popular means for business partners to exchange information.

## F

### File

A collection of data or information that has a name, called the *filename*. Almost all information stored in a computer must be in a file. There are many different types of files: *data files*, *text files*, *program files*, *directory files*, and so on. Different types of files store different types of information. For example, program files store programs, whereas text files store text.

### Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defence in protecting private information. For greater security, data can be encrypted.

**Floppy Disk**

A small, portable plastic disk coated in a magnetisable substance used for storing computer data, readable by a computer with a floppy disk drive

**Folder**

In graphical user interfaces such as Windows and the Macintosh environment, a folder is an object that can contain multiple documents. Folders are used to organize information. In the DOS and UNIX worlds, folders are called directories.

**FTP**

FTP is the abbreviation of *File Transfer Protocol*, the protocol used on the Internet for downloading and uploading files and a number of special applications can furnish FTP services for you. (However, if you are downloading through a Web page, the FTP request is set up for you by the Web page. You are usually asked where you want the downloaded file placed on your hard disk, and then the downloading transmission takes place.)

**G****H****Hacker**

A slang term for a computer enthusiast. Among professional programmers, the term *hacker* implies an amateur or a programmer who lacks formal training. Depending on how it is used, the term can be either complimentary or derogatory, although it is developing an increasingly derogatory connotation. The pejorative sense of *hacker* is becoming more prominent largely because the popular press has co-opted the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker.

**Hand-held computer**

A portable computer that is small enough to be held in one's hand. Although extremely convenient to carry, handheld computers have not replaced notebook computers because of their small keyboards and screens. The most popular hand-held computers are those that are specifically designed to provide PIM (personal information manager) functions, such as a calendar and address book. Some manufacturers are trying to solve the small keyboard problem by replacing the keyboard with an electronic pen. However, these pen-based devices rely on handwriting recognition technologies, which are still in their infancy.

**Hard disk**

A hard disk is part of a unit, often called a "disk drive," "hard drive," or "hard disk drive," that stores and provides relatively quick access to large amounts of data on an electromagnetically charged surface or set of surfaces. Today's computers typically come with a hard disk that contains several billion bytes (gigabyte) of storage.

**Hardware**

Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips. In contrast, software is untouchable. Software exists as ideas, concepts, and symbols, but it has no substance. Books provide a useful analogy. The pages and the ink are the hardware, while the words, sentences, paragraphs, and the overall meaning are the software. A computer without software is like a book full of blank pages -- you need software to make the computer useful just as you need words to make a book meaningful.

### **Home Page**

The main page of a Web site. Typically, the home page serves as an index or table of contents to other documents stored at the site. The Mater homepage is <http://www.mater.ie/>

### **Hospital Wide Access Information**

Information intended for hospital use and not external distribution.

### **HTTP**

Short for *HyperText Transfer Protocol*, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

## **I**

### **Internet**

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

### **Intranet**

A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the *firewall* surrounding an intranet fends off unauthorized access. The Mater intranet is <http://minerva.mater.ie>

### **IP Address**

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. E.g. 10.2.103.45

### **ISDN**

Abbreviation of *integrated services digital network*, an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires.

### **ISP**

Short for *Internet Service Provider*, a company that provides access to the Internet. For a monthly fee, the service provider gives you a software package, username, password and access phone number. Equipped with a modem, you can then log on to the Internet and browse the World Wide Web and USENET, and send and receive e-mail. In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company's networks to the Internet. ISPs themselves are connected to one another through *Network Access Points (NAPs)*.

## **J**

### **Java**

A high-level programming language developed by Sun Microsystems. Java is an object-oriented language similar to C++, but simplified to eliminate language features that cause common programming errors. Java is a general purpose programming language with a number of features that make the language well suited for use on the

World Wide Web. Small Java applications are called Java applets and can be downloaded from a Web server and run on your computer by a Java-compatible Web browser, such as Netscape Navigator or Microsoft Internet Explorer.

### **Java script**

A scripting language developed by Netscape to enable Web authors to design interactive sites. Javascript can interact with HTML source code, enabling Web authors to spice up their sites with dynamic content.

## **K**

## **L**

### **Laptop**

A notebook computer is a battery-powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces such as on airplanes, in libraries, temporary offices, and at meetings. A notebook computer, sometimes called a laptop computer, typically weighs less than 5 pounds and is 3 inches or less in thickness.

### **Leased Line**

A permanent telephone connection between two points set up by a telecommunications common carrier. Typically, leased lines are used by businesses to connect geographically distant offices. Unlike normal dial-up connections, a leased line is always active. In some contexts, it's called a *dedicated* line.

### **Log on**

In general computer usage, logon is the procedure used to get access to an operating system or application, usually in a remote computer. Almost always a logon requires that the user have (1) a user ID and (2) a password. Often, the user ID must conform to a limited length such as eight characters and the password must contain at least one digit and not match a natural language word. The user ID can be freely known and is visible when entered at a keyboard or other input device. The password must be kept secret (and is not displayed as it is entered). A similar procedure, called *registration*, is required to enter some Web sites.

## **M**

### **MAC Address**

Short for **Media Access Control address**, a hardware address that uniquely identifies each node of a network.

### **Macro Virus**

A type of computer virus that is encoded as a macro embedded in a document.

### **Mailbox**

An area in memory or on a storage device where e-mail is placed. In e-mail systems, each user has a private mailbox. When the user receives e-mail, the mail system automatically puts it in the mailbox. The mail system allows you to scan mail that is in your mailbox, copy it to a file, delete it, print it, or forward it to another user.

### **Mailing-List**

A mailing list is a list of people who subscribe to a periodic mailing distribution on a particular topic. On the Internet, mailing lists include each person's e-mail address rather than a postal address. Mailing lists have become a popular way for Internet

users to keep up with topics they're interested in. Many software producers and other vendors are now using them as a way to keep in touch with customers.

### **Microsoft Windows**

A family of operating systems for personal computers. In addition to Windows 3.x and Windows 95, which run on Intel-based machines, Microsoft also sells Windows NT, a more advanced operating system that runs on a variety of hardware platforms.

### **MIME**

MIME (Multi-Purpose Internet Mail Extensions) is an extension of the original Internet e-mail protocol that lets people use the protocol to exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII handled in the original protocol, the Simple Mail Transport Protocol (Simple Mail Transfer Protocol).

### **Multimedia**

The use of computers to present text, graphics, video, animation, and sound in an integrated way. Nearly all PCs are capable of displaying video, though the resolution available depends on the power of the computer's video adapter and CPU. Because of the storage demands of multimedia applications, the most effective media are CD-ROMs.

## **N**

### **Network**

A group of two or more computer systems linked together. There are many types of computer networks, including:

- **local-area networks (LANs):** The computers are geographically close together (that is, in the same building).
- **wide-area networks (WANs):** The computers are farther apart and are connected by telephone lines or radio waves.

Computers on a network are sometimes called *nodes*. Computers and devices that allocate resources for a network are called *servers*.

### **Network Interface Card or Network Card**

Often abbreviated as *NIC*, an *expansion board* you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.

### **Node**

A system connected to a network.

## **O**

### **Off-line**

Not connected. For example, all printers have a switch that allows you to turn them off-line. While the printer is off-line, you can perform certain commands like advancing the paper (*form feed*), but you cannot print documents sent from the computer.

### **Online**

Turned on and connected. For example, printers are on-line when they are ready to receive data from the computer. You can also turn a printer *off-line*. While the printer is off-line, you can perform certain tasks such as advancing the paper, but you cannot send data to it. Most printers have an on-line button you can press to turn the machine on- or off-line.

Users are considered *on-line* when they are connected to a computer service through a modem. That is, they are actually *on the line*.

### **Operating System**

The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

## **P**

### **Password**

A secret series of characters that enables a user to access a file, computer, or program. On multi-user systems, each user must enter his or her password before the computer will respond to commands. The password helps ensure that unauthorized users do not access the computer. In addition, data files and programs may require a password.

### **Peripheral devices**

Any external device attached to a computer. Examples of peripherals include printers, disk drives, display monitors, keyboards, and mice.

### **PGP**

PGP (Pretty Good Privacy) is a popular program used to encryption and decrypt e-mail over the Internet. It can also be used to send an encrypted digital signature that lets the receiver verify the sender's identity and know that the message was not changed en route.

### **PKI**

Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet. PKIs integrate digital certificates, public-key cryptography, and certificate authorities into a total, enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrolment software; integration with corporate certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

### **Point of Presence**

A point-of-presence (POP) is the location of an access point to the Internet. A POP necessarily has a unique Internet (Internet Protocol) address. Your independent service provider (Internet service provider) or online service provider (online service provider) has a point-of-presence on the Internet. POPs are sometimes used as one measure of the size and growth of an ISP or OSP.

### **Pont-to-Point Protocol**

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (Internet Protocol) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) services. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

### **Policy**

The set of laws, rules, and practices that regulate how an organization manages, protects and distributes the subject of the policy.

**POP3**

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mailbox on the server and download any mail.

**Process**

An executing program. The term is used loosely as a synonym of *task*.

**Program**

An organized list of instructions that, when executed, causes the computer to behave in a predetermined manner. Without programs, computers are useless.

**Proxy Server**

In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

**Private Key**

In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, the communicators would share a key so that each could encryption and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key. See public key infrastructure (public key infrastructure) for more information.

**PSTN**

Short for *Public Switched Telephone Network*, which refers to the international telephone system based on copper wires carrying analog voice data. This is in contrast to newer telephone networks base on digital technologies, such as ISDN and FDDI.

**Public Information**

Information that is available for/or distributed to the general public either regularly or upon request.

**Public Key**

A public key is a value provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encryption messages and digital signature. The use of combined public and private keys is known as *asymmetric* cryptography. A system for using public keys is called a public key infrastructure (public key infrastructure).

**Q****R****Reboot**

To restart a computer. In DOS, you can reboot by pressing the Alt, Control and Delete keys simultaneously.

**Remote Access**

The ability to log onto a network from a distant location. Generally, this implies a computer, a modem, and some remote access software to connect to the network.

The remote access software dials in directly to the network server. The only difference between a remote host and workstations connected directly to the network is slower data transfer speeds.

### **Resource**

Generally, any item that can be used. Devices such as printers and disk drives are resources, as is memory, applications and data.

### **Risks**

Can be classified as employee error, other accidents, long-term system failures, natural disasters and criminal or malicious action. Such events could result in damage to or loss of information resources, loss of data accuracy or integrity, or interruption of normal data processing.

## **S**

### **Security**

Freedom from risk or danger. Safety and the assurance of safety.

Refers to techniques for ensuring that data stored in a computer cannot be read or compromised. Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

### **Shortcut**

In Windows 95 and Windows 98 a special type of file that points to another file or device. You can place shortcuts on the desktop to conveniently access files that may be stored deep in the directory structure. Double-clicking the shortcut icon is the same as double-clicking the actual file. You can control how a shortcut appears by naming it anything you want and associating a particular icon with it.

### **SMTP**

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail.

### **Software**

Software is a general term for the various kinds of program used to operate computer and related devices. (The term hardware describes the physical aspects of computers and related devices.) Software is often divided into application software (programs that do work users are directly interested in) and system software (which includes operating system and any program that supports application software).

### **SPAM**

Spam is unsolicited e-mail on the Internet. Spam is any email you did not ask for, but get from people you do not know who want to sell something to you. It is not sent only to you, however, but to every single email address the spammer can get hold of.

### **SSL**

Short for *Secure Sockets Layer*, a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. By convention, Web pages that require an SSL connection start with *https:* instead of *http:*.

## **T**

**Tape**

In computers, tape is an electromagnetic storage medium that typically is both readable and writable. A tape drive is the device that positions, writes from, and reads to the tape. Tapes come in a variety of sizes and formats.

**Task**

In computer programming, a task is a basic unit of programming that an operating system controls. Depending on how the operating system defines a task in its design, this unit of programming may be an entire program or each successive invocation of a program

**Telecommunications**

Refers to all types of data transmission, from voice to video.

**Terminal**

A computer terminal or microcomputer, which allows access to any administrative computing system.

**Trojan Horse**

A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer virus. A Trojan horse can be considered a virus if it is widely redistributed. The term comes from Homer's *Iliad*. In the Trojan War, the Greeks presented the citizens of Troy with a large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city.

**U****USENET News**

Is a worldwide bulletin board system that can be accessed through the Internet or through many online services. The USENET contains more than 14,000 forums, called *newsgroups* that cover every imaginable interest group. It is used daily by millions of people around the world.

**URL**

A URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. Using the World Wide Web's protocol, the Hypertext Transfer Protocol (Hypertext Transfer Protocol) the resource can be an HTML page (like the one you're reading), an image file, a program such as a common gateway interface application or Java applet, or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer. On the Web (which uses the Hypertext Transfer Protocol), an example of a URL is:

<http://www.mater.ie/depts>

which describes a Web page to be accessed with an HTTP (Web browser) application that is located on a computer named [www.mater.ie](http://www.mater.ie). The specific file is in the directory named /depts.

**Username**

A name used to gain access to a computer system. Usernames, and often passwords, are required in multi-user systems. Usernames are also required to access some bulletin board and online services.

## V

### **Virus**

A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Most viruses can also replicate themselves. All computer viruses are manmade. Viruses can be transmitted by sending them as attachments to an e-mail note, by downloading infected programming from other sites, or be present on a diskette or CD. The source of the e-mail note, downloaded file, or diskette you've received is often unaware of the virus.

## W

### **WallBox**

A specific place for being physically connected to the network.

### **Web Page**

A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

### **Web Site**

A site (location) on the World Wide Web. Each Web site contains a home page, which is the first document users see when they enter the site. The site might also contain additional documents and files. Each site is owned and managed by an individual, company or organization.

### **World Wide Web**

A technical definition of the World Wide Web is: all the resources and users on the Internet that are using the Hypertext Transfer Protocol (Hypertext Transfer Protocol). There are several applications called Web browsers that make it easy to access the World Wide Web; Two of the most popular being Netscape Navigator and Microsoft's Internet Explorer.

### **Windows**

When spelled with a capital W, Windows is short for [\*Microsoft Windows\*](#).

## X

## Y

## Z

### **ZIP drive**

A high-capacity floppy disk drive developed by Iomega Corporation. Zip disks are slightly larger than conventional floppy disks, and about twice as thick. They can hold 100 MB of data.