



## Contents:

<b>1</b>	<b>Information Security Supporting Policies.....</b>	<b>4</b>
1.1	Introduction .....	4
1.2	Definitions .....	4
<b>2</b>	<b>Network Security Policy .....</b>	<b>5</b>
2.1	Network Administration Roles and Responsibilities .....	6
2.2	Connection to the College Network .....	6
2.3	Wireless Networking .....	7
2.4	Server Connectivity .....	7
2.5	Network Access Controls .....	7
2.6	Connection of Privately Owned Equipment .....	8
2.7	Network Administration .....	8
2.8	Use of Network Facilities .....	9
<b>3</b>	<b>Internet Use Policy .....</b>	<b>10</b>
3.1	Conditions Governing use of College Internet Facilities .....	10
<b>4</b>	<b>Email Use Policy .....</b>	<b>12</b>
4.1	Conditions governing use of College E-mail facilities .....	12
4.2	E-mail and Data Protection .....	14
4.3	Email and Copyright .....	14
4.4	E-mail and Privacy .....	14
<b>5</b>	<b>Password Policy .....</b>	<b>15</b>
5.1	Issue of accounts and passwords .....	15
5.2	Password Sharing Prohibition .....	15
5.3	Writing Passwords Down and Leaving Where Others Could Discover .....	15
5.4	Password Changes .....	15
5.5	Minimum Password Length .....	15
5.6	Complex Passwords Required .....	16
5.7	Cyclical Passwords Prohibited .....	16
5.8	User-Chosen Passwords Must Not Be Reused .....	16
5.9	Password Ageing .....	16
5.10	Limit on Consecutive Unsuccessful Attempts to Enter a Password .....	16
5.11	Password History .....	16
5.12	System Compromise .....	16
5.13	Storage of Passwords in Readable Form .....	17
5.14	Changing Vendor Default Passwords .....	17
5.15	Encryption .....	17
5.16	Misuse of Passwords .....	17
<b>6</b>	<b>Virus and Spam Policy .....</b>	<b>17</b>
6.1	Virus Prevention - Network Users Responsibilities .....	18
6.2	Where a virus is detected by a User .....	18
6.3	Unsolicited Email (Spam) User Responsibilities .....	18
6.4	Virus and spam Prevention - Administrative responsibilities .....	19
<b>7</b>	<b>Software Security Policy .....</b>	<b>19</b>
7.1	Approval by the Information Policy Committee .....	20
7.2	Software Security Standards .....	20
7.3	Purchasing Software .....	20
7.4	Software Development .....	21
7.5	College Data .....	21
7.6	E-Payment or Storage of Credit / Debit Card Numbers .....	22
7.7	Username and Password Authentication .....	22
7.8	Change Control .....	22
7.9	Encryption .....	22
7.10	Software Installation, Configuration and Updates .....	23
7.11	Licensing .....	23



7.12	Copyright .....	24
7.13	Breach of Policy .....	24
<b>8</b>	<b>Data Backup Policy .....</b>	<b>24</b>
8.1	Best Practice Backup Procedures .....	24
8.2	Responsibility for Data backup .....	25
8.3	Legal Requirements .....	25
8.4	Desktop Backups .....	25
<b>9</b>	<b>Disaster Recovery Policy .....</b>	<b>26</b>
9.1	Published Disaster Recovery Plan/Procedures .....	26
9.2	User Responsibilities .....	26
9.3	Best Practice Disaster Recovery Procedures .....	26
<b>10</b>	<b>Remote Access Policy .....</b>	<b>27</b>
10.1	Permitted remote access connections .....	27
10.2	Methods of Remote connection .....	27
10.3	Non-standard remote access connections .....	27
10.4	Protecting Remote Access Credentials .....	28
10.5	Username/Password Authentication .....	28
10.6	Remote Access Hosts .....	28
10.7	All Individuals/groups granted remote access connection Privileges .....	28
10.8	College Staff or Students providing remote access to Third parties .....	28
10.9	Third Parties .....	29
<b>11</b>	<b>Third Party Access .....</b>	<b>29</b>
11.1	Scope .....	29
11.2	Permitted Third Party Access .....	29
11.3	Access Requests .....	29
11.4	Security Conditions in Third Party contracts .....	30
11.5	Confidentiality .....	30
11.6	Unique Authentication .....	31
11.7	Host Security .....	31
11.8	Remote Access by Third Parties .....	31
<b>12</b>	<b>Incident Response and Misuse of IT Facilities Policy .....</b>	<b>31</b>
12.1	Incident Reporting .....	32
12.2	Reporting an incident .....	32
12.3	Documentation .....	32
12.4	Disabling Accounts/Network Connections .....	32
12.5	Communication / Control .....	32
12.6	Obtaining Evidence .....	33
12.7	Preserve Configuration .....	33
12.8	Query External Resources .....	33
12.9	Liaison with third parties .....	33
12.10	Follow-up Actions .....	33
12.11	Records of Security Incidents .....	34
<b>13</b>	<b>Misuse of College IT Facilities .....</b>	<b>34</b>
13.1	Staff and Third Parties .....	34
13.2	Students .....	34
13.3	Student Disciplinary Offences .....	34
<b>14</b>	<b>Legal Compliance Guidelines .....</b>	<b>35</b>
14.1	Relevant legislation .....	35
14.2	Confidentiality .....	35
14.3	Unauthorised Access Attempts .....	35
14.4	HEANET Acceptable Use Policy .....	36
14.5	Copyright, Intellectual Property and Patents. ....	36
14.6	Libel .....	36
14.7	Protection of Minors .....	36
14.8	Sexually Explicit Material .....	37



14.9	E-commerce Act .....	37
14.10	Unsolicited Commercial Emails .....	37
14.11	Freedom of Information .....	37
14.12	Data Protection Act .....	38
14.13	College Compliance with Data Protection Act .....	39
14.14	Subject Access Request under Data protection legislation .....	39
14.20	Data Protection- Future Developments .....	41
14.21	Data Protection - User compliance .....	41
14.22	Breach of Data Protection Act .....	42



## 1 Information Security Supporting Policies

### 1.1 Introduction

This document supports and expands on the published College Information Security Policy as approved by the College Board.

All staff and students of the College and all other users authorised by the College are required to familiarise themselves with and comply with these policies.

### 1.2 Definitions

#### Network Users

Network users are defined as all College staff, students or third parties with either a College owned or personally owned computer or other device used to connect to the College network or a username and password or other type of authentication allowing access to the College network.

#### Autonomous Managed Networks (AMN's)

The autonomously managed networks (AMN's) are separate logical and physical networks created to address specific needs of a localised user population. They are operated under licence by the IPC and managed by dedicated full time and suitably qualified staff.

#### Autonomous Network Managers

Each AMN as defined above appoints a named individual as the AMN manager this person is responsible for authorising requests locally and liaising with Information Systems Services.

#### Third Parties

Third parties are defined as any individual, group contractor, vendor or agent not registered as a College staff member or student.

#### Third Party Access

Third party Access is defined as all local or remote access to the College Network or devices attached to the College Network for any purpose.

#### Software

Software is defined as any operating system, application, database or other IT system that is used to collect process or store data in an electronic format.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	4 of 42



## College staff

Defined as all current registered employees (full time and part time) of Trinity College Dublin.

## Students

Defined as all currently registered students of Trinity College Dublin.

## Third Parties

Defined as any individual, group contractor, vendor or agent not registered as a College staff member or student who is granted access to the College network or to College systems or College data.

## Software

Software in this policy is defined as any operating system, application, database or other IT system that is used to collect process or store data in an electronic format.

## College Information

Defined as any data pertaining to College staff, students, or activities. Additionally any data collected by College or other bodies or currently centrally managed by the Management Information n systems (MIS) group in Information Systems Services.

## Personal Information

Defined as personal data pertaining to any individual e.g. Name, address, age,

## Sensitive data

Is defined as financial data, sensitive teaching or research data or personal data relating to individuals.

## **2 Network Security Policy**

The Trinity College IT network consists of an interconnection of approximately 10,000-networked devices. These include computers, printer's network cables and other networking equipment. The College depends heavily upon its IT network for research, teaching and administrative activities. It is essential that the stability, integrity and security of the College IT network be safeguarded.

This policy defines the College regulations regarding access to the College Network. All Network Users must comply with the following policy statements:

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	5 of 42



### 2.1 *Network Administration Roles and Responsibilities*

Information Systems Services are responsible for the administration of the College backbone network and primary software domains.

The administration of the College network including, network connections, services, addressing and design is the responsibility of the Information Systems Services Network Manager and delegated agents.

Additional authorised autonomous managed networks exist which are connected to the College Backbone at an authorised connection point.

Authorisation to operate an autonomous network must be sought from the information Policy Committee. The information Policy committee will issue a licence detailing the conditions of operation for the autonomous network. All licenses must be renewed annually.

Multiple authorised software domains exist within the College network. The administration of these domains including user accounts and other access controls is the responsibility of the appointed administrator.

### 2.2 *Connection to the College Network*

Connection to and use of College network facilities is dependent on compliance with all published Information Systems Services and College Policies.

All equipment connected to the College network must conform to the appropriate standards as set periodically by Information Systems Services and Autonomous Network Managers and run only across the backbone using protocols supported by the College.

Only Information Systems Services or authorised Autonomous Network Managers may connect devices to the College Network.

Side-entry connections to the College network, for example via modem connection to the asynchronous port of a workstation, or via wireless devices are permitted only with the permission of Information Systems Services, or the relevant Autonomous Network Manager.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	6 of 42



### 2.3 Wireless Networking

The Director of Information Systems Services or their designee is responsible for providing a secure and reliable campus network to support the mission of the University. Under this broad responsibility, the following campus-wide wireless policies apply:

- Only hardware and software consistent with wireless standards approved by the Information Systems Services and the Wireless Community Committee shall be used for wireless access points.
- All wireless access points shall be registered with Information Systems Services. In the event that a wireless device interferes with other equipment, the Director of IS Services or designee shall resolve the interference as determined by use priority.
- Deployment and management of wireless access points in common areas of the campus is the responsibility of Information Systems Service.

### 2.4 Server Connectivity

The connection and use of a computer running Server operating system software or otherwise functioning as a server must be authorised by information Systems Services or an appropriate Autonomous Network Manager.

All Servers must have a defined administrator who is responsible for:

- Server administration and maintenance
- Server security including but not limited to data backup, access control, operating system and application updates and security patches

College reserves the right to bar access to Information Servers containing material considered illegal or likely to bring the College into disrepute. The College also reserves the right to take disciplinary action in these circumstances.

The College will not be liable for any loss or damage suffered by the Information Owner as a result of barring access to or removal of material. Where the Information Owner considers that the College has acted disproportionately or inappropriately in barring access to and/or removing the material then s/he has the right of appeal through the normal College grievance procedures.

In the event that a server is causing an unacceptable level of interference with the operation of the College network out of normal hours and the owner/administrator cannot be contacted Information Systems services or the Autonomous Network Manager may take action to disconnect the Server from the network.

### 2.5 Network Access Controls

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	7 of 42



Access to College network and facilities is restricted to fully authorised College users. Users are required to login to an authorised domain using a secure login-name/password combination. Additional authentication mechanisms may be required if Information Systems Services, or Autonomous Network Managers deem it necessary.

Information Systems Services and Autonomous Network Managers must ensure that only authorised College users have access to the network from their systems.

### 2.6 *Connection of Privately Owned Equipment*

Students may connect computing equipment to the College network only with the permission of Information Systems Services. Such systems are then subject to all the statutory and College rules/regulations/policies currently in force and which are applicable to the fields of computer information systems.

Students may connect private equipment using the NAC self service network in the manner outlined by Information Systems Services on the official website.

In general users may connect private equipment to the network by following the procedures outlined by Information systems Services. All private equipment must meet minimum hardware/software requirements and pass appropriate security checks as defined and updated by Information Systems Services.

### 2.7 *Network Administration*

All network addresses; including IP addresses, must be allocated and administered by Information Systems Services or authorised Autonomous Network Managers.

Information Systems Services must be informed of any proposed physical re-organisation to the network. This includes requests for extra cabling or the insertion of wireless networking devices within an academic or administrative area. All requests for physical connections to the College backbone must be directed to the Information Systems Services Helpdesk.

Information Systems Services, and Autonomous network managers may, on behalf of the College, and subject to appropriate consultations, restrict excessive use of the backbone bandwidth.

In the event of unacceptable network events occurring on the network, Information Systems Services, and Autonomous network managers have the right to gain access to and inspect the configuration of devices or equipment on that network and to request the immediate removal of any devices or equipment that it believes could be the source of the problem.

In the event of unacceptable events on a network causing problems on another part of the College

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	8 of 42





network or on an external network, Information Systems Services has the right to disable any part of the network as necessary, in order to remove the source of the problem. While every effort will be made to contact the system owner, Head of academic or administrative are and/or other appropriate persons, this may not always be possible. All services will be reconnected at the first opportunity.

### 2.8 Use of Network Facilities

All Network Users must comply with the following conditions of use which apply to the College network and all attached devices:

- Use of the Network facilities including but not limited to the network, workstations, printers and the facilities associated with it e.g. software, data, email, world wide web (www), bulletin boards, data is subject to the College's [Code of Conduct](#).
- All data/programs created/owned/stored by the user on or connected to College Network facilities may subjected to inspection by the Director of Information Systems Services or nominated agent in the instance of suspected wrongdoing. Should the data/programs be encrypted the User shall be required to provide the decryption key to facilitate decryption of the data/programs. Where evidence is found of misuse or of the illegal use of material it will be subject to removal/deletion.
- Users should not use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction or access to any College or Network facilities.
- Users should not display, store or transmit images or text which could be considered offensive e.g. material of a sexual, pornographic, paedophilic, sexist, racist, libellous, threatening, defamatory nature, of a terrorist nature or likely to bring the College into disrepute.
- Users must not forge email signatures and/or headers, initiate and/or forward 'chain' or 'junk' or 'harassing' mail.
- Users should comply with all relevant IT legislation as outlined in the Information Systems Security Policy.
- When holding data on computers about living individuals users must register the data and its uses, according to College procedures and in accordance with the Data Protection Act.
- Other than any statutory obligation, the College will not be liable for any loss, damage or

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	9 of 42



inconvenience arising directly or indirectly from the use of, or prevention of use of, any Network facility provided and/or managed by the College.

- Whilst the College takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data, personal or other. The same applies to other IT material submitted to or processed on facilities provided or managed by the College or otherwise deposited at or left on its premises.
- A user's name, address, photograph, status, e-mail name, login name, alias, Staff/Student number and other related information will be stored in electronic form for use for administrative and other operational purposes.
- Breaking these conditions may lead to College disciplinary procedures being invoked, with penalties, which could include suspension from the use of all College computing facilities for extended periods and or fines. Serious cases may lead to expulsion or dismissal from the College and may involve civil or criminal action being taken against the user.

### 3 Internet Use Policy

The Internet is recognised as an important communication and research tool for Trinity College network users. This policy details standards for the secure use of Internet facilities for College purposes, including teaching, research and administration.

#### 3.1 *Conditions Governing use of College Internet Facilities*

All users must adhere to the following when using College facilities to connect to the Internet:

- Access to the Internet is provided for Trinity College purposes and must not be abused for personal use.
- Commercial use, which is not connected to or approved by the College, is strictly prohibited and will result in disciplinary procedures,
- Internet access in College is available only via the College infrastructure. Users should not connect to the Internet via a dial-up ISP account on College computers connected to the network.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	10 of 42



- Users are expected to act ethically and responsibly in their use of the Internet and to comply with the relevant national legislation, the College Information Security policy, regulations and codes of practice. Users must not post messages on newsgroups or chat areas that are likely to be considered abusive, offensive or inflammatory by others.
- Users must not use the College Internet connection to scan or attack other individuals/devices/organisations. The use of port scanners or other hacking tools unless used as part of an approved course of study is strictly prohibited.
- Users should be aware that the public nature of the Internet dictates that the confidentiality and integrity of information cannot normally be relied upon.
- Where a requirement exists to send or receive confidential or commercially sensitive data over the Internet, a security mechanism recommended by the IT Security Specialist should be used.
- Passwords used for Internet services should not be the same or similar to passwords used for services accessed within College. This is to prevent passwords that grant access to College IT resources being sent out on the Internet in clear text where any Internet user can potentially see them. Similarly, any username used for the Internet services should not be the same or similar to a College username.
- Software copyrights and licence conditions must be observed. Only licensed files or software may be downloaded from the Internet.
- The use of the College Internet Connection to download or distribute copyright material using peer-to-peer applications is strictly prohibited. Information Systems Services reserve the right to disconnect any machines involved in illegal file distribution from the College network.
- All devices connected to the Internet must be equipped with the latest versions of anti-virus software, which has been both approved and supplied by College.
- All forms of data received over the Internet should immediately be virus checked.
- All forms of data transmitted from College over the Internet should be virus checked in advance.
- Data, which has been compressed or encrypted, should be decompressed or decrypted as required before virus checking.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	11 of 42



- All security incidents involving Internet access must be reported to the [IT Security Officer](#).

### 4 Email Use Policy

E-mail is recognised as an important communication tool for Trinity College network users. This document details standards for the secure use of Internet facilities for College purposes, including teaching, research and administration

#### 4.1 *Conditions governing use of College E-mail facilities*

All users must adhere to the following when using College E-mail facilities:

- Users are expected to act ethically and responsibly in their use of e-mails and to comply with the relevant national legislation, the College Information Security policy, regulations and codes of practice.
- Discrimination, victimisation or harassment on the grounds of gender, marital status, family status, sexual orientation, religious belief, age, disability, race, colour, nationality, ethnic or national origin is against College Policy. Users must not bully, hassle or harass other individuals via e-mail. Users must not send messages that are likely to be considered abusive, offensive or inflammatory by the recipient/s.
- All users should regard all e-mails sent from College facilities as first, representing the College and, secondly, representing the individual. Users should be civil and courteous. Users should not send e-mail, which portrays the College in an unprofessional light. The College is liable for the opinions and communications of its staff and students. Any e-mail involved in a legal dispute may have to be produced as evidence in court.
- All users should do their best to ensure that email content is accurate, factual and objective especially in relation to individuals. Users should avoid subjective opinions about individuals or other organisations.
- Users should be aware that e-mails can easily be forwarded to other parties. Users should assume that anyone mentioned in e-mail could see it or hear about it or he/she may, under data protection or other law, be entitled to see it.
- All users should be aware that. it is possible for the origin of an e-mail to be easily disguised and for it to appear to come from someone else.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	12 of 42



- Users must not use a false identity in e-mails.
- Users must not create or forward advertisements, chain letters or unsolicited e-mails e.g. SPAM
- All users should protect data displayed on their monitor. E.G by locking their office door or by locking their workstation or using a screen saver in password-protected mode when leaving their desk. This is in order to prevent unauthorised individuals from using the workstation to send an e-mail, which will appear to originate from the user.
- All users should exercise caution when providing their e-mail address to others and be aware that their e-mail address may be recorded on the Internet.
- All users should be cautious when opening e-mails and attachments from unknown sources as they may be infected with viruses.
- All users must have up-to-date College approved anti-virus software installed and operational on the computer that they access their email on.
- All emails or attachments that are encrypted or compressed should be decrypted or decompressed and scanned for viruses by the recipient.
- Users should be aware that e-mails may be subject to audit by Information Systems Services to ensure that they meet the requirements of this policy. This applies to message content, attachments and addressees and to personal e-mails.
- As part of the College's standard computing and telecommunications practices, email systems and the systems involved in the transmission and storage of e-mail messages are normally "backed up" centrally on a routine basis for administrative purposes. The back-up process results in the copying of data, such as the content of an e-mail message, on to storage media that may be retained for periods of time and in locations unknown to the originator or recipient of an email. The frequency and retention of back-up copies vary from system to system. However, this back-up is for College administrative purposes only and it is the user's own responsibility to back-up any of their e-mails they wish to retain for future reference.
- All security incidents involving E-mail should be reported to the [IT Security Officer](#).

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	13 of 42



### 4.2 *E-mail and Data Protection*

All College users should be aware that E-mail falls under the scope of the data protection act. Under this legislation the email originator, all email recipients and any persons named in the e-mail are entitled to view the information about them and if it is incorrect they are entitled to have it corrected.

Home or personal use has a “domestic exemption” from data protection law, but the College has no such exemption even for personal e-mails if they originate from the College network. In addition, e-mails can constitute publication for the purpose of the law of libel.

Additionally any information, which Trinity Users collect via the Internet such as personal or financial details collected via Internet forms or surveys, fall under the Data protection Act.

All users must ensure that the methods of collecting processing and storing information in this way comply with the College policies the data protection act and any other relevant legislation.

### 4.3 *Email and Copyright*

Copyright law stops other people from using and abusing individual's original work. Users should bear in mind, therefore, that:

- E-mail messages are creative works and therefore are copyrighted.
- All e-mail messages sent by a user are copyrighted to the user (or the College).
- Users do not have to register this copyright - it exists automatically.
- When Users post to a public list they do not lose copyright, but the message may be archived forwarded to other lists or quoted by others.
- Messages sent to a list should not be quoted out of context, changed or reworded or mis-attributed.
- Software or files downloaded from the Internet may be protected by copyright restrictions.

### 4.4 *E-mail and Privacy*

Data users must assume that all e-mail or Internet communications are not secure unless encrypted and they should not send via e-mail any information, which is confidential. Users may not, under any circumstances, monitor, and intercept or browse other users' e-mail messages unless authorised to do so. Network and computer operations personnel, or system administrators, may not monitor other users' e-mail messages other than to the extent that this may occur incidentally in the normal course of their work.

The College reserves the right to access and disclose the contents of a user's e-mail messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. The

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	14 of 42



College reserves the right to demand that encryption keys, where used, be made available so that it is able to fulfil its right of access to a user's e-mail messages in such circumstances.

### 5 Password Policy

Username and passwords are utilised in Trinity College Dublin to facilitate access to College IT resources. They also protect College data from access from unauthorised individuals both internally (other staff students) and externally (hackers).

This policy applies to all College Staff, Students, or Third parties who are issued with usernames and passwords for any College IT System or device.

This policy applies to all username and password pairs on all devices, systems and applications that are part of the College network that provide access to College owned information.

#### 5.1 *Issue of accounts and passwords*

All system and application accounts and passwords must be issued by Information Systems Services or an Autonomous Network Manager. Once a password has been issued full responsibility for that account and associated password passes to the user.

#### 5.2 *Password Sharing Prohibition*

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to responsibility for actions that the other party takes with the password. Where a user is found to have given the use of a username or password to a third party disciplinary measures will be implemented.

#### 5.3 *Writing Passwords Down and Leaving Where Others Could Discover*

Passwords must not be written down and left in a place where unauthorised persons might discover them.

#### 5.4 *Password Changes*

Password changes must only be made when requested in person by the appropriate individual or when requested by a trusted party as defined by Information Systems Services. No exceptions to this policy are allowed.

#### 5.5 *Minimum Password Length*

The length of passwords must always be checked automatically at the time that users construct or select them. All IT systems must require passwords of at least six (6) characters.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	15 of 42



### 5.6 *Complex Passwords Required*

All computer system users must choose passwords that cannot be easily guessed. For example, a car license plate number, a spouse's name, or an address must not be used. This also means that passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, and slang must not be used.

### 5.7 *Cyclical Passwords Prohibited*

Users must not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users must not employ passwords like "JANUARY" in January, "FEBRUARY" in February, etc.

### 5.8 *User-Chosen Passwords Must Not Be Reused*

Users must not construct passwords that are identical or substantially similar to passwords that they had previously employed.

### 5.9 *Password Ageing*

Passwords should be changed periodically. Network managers, system administrators or application administrators should select an appropriate time frame for changing passwords. The IT security officer can give advice.

### 5.10 *Limit on Consecutive Unsuccessful Attempts to Enter a Password*

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After a defined number of unsuccessful attempts to enter a password (usually between 3 and 8 per hour), the involved user account must be either (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three (3) minutes, or (c) if dial-up or other external network connections are involved, disconnected.

### 5.11 *Password History*

A password history must be maintained for all domain level. This history file should be used to prevent users from reusing passwords. The history file should minimally contain the last 7 passwords for each username.

### 5.12 *System Compromise*

Whenever an unauthorised party has compromised a system, Information Systems Services or the relevant Autonomous network manager or application administrator must immediately change every password on the involved system. Even suspicion of a compromise likewise requires that all

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	16 of 42





passwords be changed immediately. Under either of these circumstances, a trusted version of the operating system and all security-related software must also be reloaded. Similarly, under either of these circumstances, all recent changes to user and system privileges must be reviewed for unauthorised modifications.

### 5.13 *Storage of Passwords in Readable Form*

Passwords must not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorised persons might discover them.

### 5.14 *Changing Vendor Default Passwords*

All vendor-supplied default passwords e.g. default passwords supplied with routers, switches or software such as operating systems and databases must be changed before any computer or communications system is used.

### 5.15 *Encryption*

Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over communications system.

### 5.16 *Misuse of Passwords*

Any abuse of passwords must be reported to IT Security who will decide on what follow-up action to take. Passwords must always be changed if it is known or suspected that another person has become aware of the password. Where a third party is found in possession of a users password that account will be disabled. In this situation the valid user should report to the [IT Security Officer](#).

## 6 **Virus and Spam Policy**

Computer viruses impact productivity, incur financial costs and can result in the compromise or loss of data and reputation.

Viruses can originate from a range of sources, spread rapidly, and require a comprehensive approach to ensure the risk they pose is effectively managed. This comprehensive approach requires the full co-operation of all Trinity College Staff and Students.

This Anti-Virus and Anti-Spam Policy and outlines the overall approach adopted by the College as well as individual responsibilities. All Trinity College network users have a responsibility to protect their systems from virus infection and follow the guidelines on spam email as outlined below:

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	17 of 42



### 6.1 *Virus Prevention - Network Users Responsibilities*

- All users have a responsibility to protect any device, which they use which connects to the College network by ensuring that they have the installed the correct anti-virus product for their area and that it is up-to-date. This relates to College owned machines and users private machines where the machines are used to access the College network.
- Users must not try to install an unapproved anti-virus product, or try to alter the configuration or disable the existing anti-virus product.
- Users must install when requested by Information Systems Services or their Autonomous Network Manager any software, which is for the prevention of or monitoring of virus infections.
- Users must ensure that all relevant software security updates are applied to their computer. Users are advised to use the Windows update service for all Microsoft operating systems, and the equivalent update service for other types of operating system.
- Users must scan their hard drives regularly for viruses.
- Users should not open suspicious emails or attachments whether solicited or unsolicited from unknown or unusual sources.
- Users should scan all software or other content that they download from the Internet for viruses.
- Users should exercise caution when downloading software from the Internet and only install software from reputable Internet sites.

### 6.2 *Where a virus is detected by a User*

- All users must respond to any virus infection detection indicated by their anti-virus software.
- In the event that a user is unable to clean or remove an infected file they should disconnect their PC from the College network by removing the network cable and inform their Autonomous Network Manager or the Information Systems Services Helpdesk of the problem immediately.
- All users should be alert to the possibility of a virus and report any suspicious behaviour to their Autonomous Network Manager or the Information Systems Services Helpdesk immediately.

### 6.3 *Unsolicited Email (Spam) User Responsibilities*

- Users should exercise caution when divulging their College Email account to third parties. Some organisations may provide your email address to parties involved in sending unsolicited emails (Spam), which may result in increased volumes of spam email being sent to your account.
- Information Systems Services provide a Spam filtering service for users of the College email system. All users should report any spam that they receive using the method advised by Information Systems Services on the website in order to improve the overall efficiency of the system.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	18 of 42



- It is strictly prohibited for any user to use College network resources to distribute unsolicited email (E.G. Spam)

### 6.4 Virus and spam Prevention - Administrative responsibilities

Information Systems Services, and Autonomous Network managers must:

- Select an effective desktop anti-virus product. This product must be licensed and made available to all users connecting to the College network.
- Monitor systems regularly for devices that do not have anti-virus software installed or have incorrect anti-virus products or settings.
- Provide a central point of contact to College users for anti-virus matters.
- Keep abreast of potential viruses that may affect the College.
- Promote awareness of anti-virus issues amongst users.
- Monitor desktop systems for indications of virus infection using available tools (E.G the Epol administration console.)
- Follow up on and evaluate any virus reports from users and make recommendations which may include informing users of the problem by email alert, intranet, etc
- During a virus outbreak incident, provide whatever assistance is required to disinfect the virus and prevent propagation.
- In the event of an incident the official source of updated information will be the Information Systems Services website.
- Information Systems Services and Autonomous Network managers running approved College email systems must scan all incoming and outgoing email at the mail gateway for viruses using a reputable virus scanning product. This is to prevent mass propagation of viruses through email systems.
- Information Systems Services and Autonomous Network managers running approved College email systems must offer a high quality spam filtering service to all users.

## 7 Software Security Policy

Software is widely used by Trinity College Dublin to process, manipulate and store data owned by the College. It is essential that all software meet minimum-security standards to ensure the integrity and security of College data.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	19 of 42



This policy applies to all College staff, students or third parties who purchase or develop software that is used on the College network or installed on any device connected to the College network or used to collect, store or process College data. This policy applies to all software purchased with private resources as well as College funds.

Particular care should be taken when purchasing or developing a major system that is to be used to process or store College data.

The responsibility for ensuring that software meets security requirements falls to the individual or group purchasing installing and configuring the product.

Where an individual does not have the required expertise to ensure that the product meets requirements advice should be sought from the IT Security Officer or Information Systems Services.

### *7.1 Approval by the Information Policy Committee*

All College users should note that proposals for new or replacement information systems are subject to approval by the Information Policy Committee. Information on submission of project proposals and committee meeting dates is available from the Information Systems Services website.

### *7.2 Software Security Standards*

All software must comply with the following standards:

- All software must protect College and personal information from unauthorised disclosure (confidentiality and privacy).
- All software must protect College and personal information from unauthorised modification (integrity).
- All software must protect College and personal information and processing services from disruption and destruction (availability).
- All software must contain controls that can ensure that individuals can be held responsible for their actions (accountability and non-repudiation).

### *7.3 Purchasing Software*

Any Staff member, Student or Third party purchasing software to be used on the College network or to process data owned by College must ensure that:

- The software meets minimum standards as detailed in section 1.3
- The software is tested to ensure that the security criteria as defined in section 1.3 are met.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	20 of 42



- The software is configured correctly and securely and that all relevant security features are enabled.
- The software meets licensing criteria as detailed in section 4 of this policy document.
- That provision is made for providing ongoing maintenance for the software either by the manufacturer or a dedicated system administrator.
- Physical or logical access should only be given to vendors for support purposes when necessary. Only approved secure methods of access should be used. (The IT Security officer can advise on suitable methods) The vendor must sign a third party access form and the vendors activities should be monitored/logged.

### 7.4 Software Development

Any Staff member, Student or Third party developing software to be used on the College network or to process data owned by College must ensure that:

- The software meets minimum standards as detailed in section 1.3
- The software is tested a professional manner to ensure that all security controls are effective. Documentation supporting this must be made available to IT Security Officer, Director of Information Systems Services, Director of MIS, or College Network Manager on request.
- Software development and testing is carried out in a separate environment from the live environment.
- Adequate controls are in place over any test data, which is used in the testing process.
- That provision is made for ongoing maintenance of the software

### 7.5 College Data

Any Staff member, Student or Third party purchasing or developing software for the purpose of gathering, processing or storing sensitive College information such as financial data, sensitive teaching or research data or personal data relating to individuals must ensure:

- That the software meets the criteria as defined in section 1.3
- That they are able to provide documentation of security controls in place.
- That they are able to provide evidence of the effectiveness of those controls gained through proper testing exercises on request from the IT Security Officer, Director of Information Systems Services or the relevant Network Manager or Systems administrator.
- Where sensitive data (E.G financial data, sensitive teaching or research data or personal data relating to individuals) is to be stored in electronic format that the College has insurance to cover any incident such as theft of the data, which may occur while the data is stored electronically.
- That they are not duplicating data already held in central College databases (e.g. Student and Staff details) or creating systems which duplicate services already provided by existing systems

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	21 of 42



### 7.6 *E-Payment or Storage of Credit / Debit Card Numbers*

Users intending to purchase or develop systems intended for e-payment or the collection and/or storing credit card numbers and associated information are alerted to the following special security considerations:

- Under most merchant agreements the issuing Bank will wish to approve any proposed system before it goes into operation.
- College has no insurance cover for the theft of credit card numbers from the College network. Thus in the case of a security breach College would have a financial liability.

In the light of these issues the IT Security recommendation is to use an accredited third party provider for such systems. This ensures that the critical credit card data is neither stored nor transmitted on the Trinity College Network. For more information please contact the IT Security Officer.

### 7.7 *Username and Password Authentication*

Packages, which use username and password authentication, must conform to '005 Passwords Standards Policy.doc'

### 7.8 *Change Control*

In order to minimise the corruption of information systems there should be strict control over the implementation of changes to software installations.

Where appropriate (which will generally be for larger systems) formal change control procedures should be enforced to ensure that security procedures are not compromised and that formal agreement and approval for any change is obtained. This should include:

- Authorisation of request for change.
- Risk assessment of change.
- User Acceptance Testing.
- Relevant management sign-off.
- Information Security sign-off.
- Rollback procedures in the event that the promotion failed.
- Documentation of the above

### 7.9 *Encryption*

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	22 of 42



If sensitive data (E.G financial data, sensitive teaching or research data or personal data relating to individuals) is to be transmitted over any external communication network, it must be sent in encrypted form. However encryption processes must not be used for College information unless the IT Security Officer first approves the process.

It may also be appropriate to use encryption where sensitive data is transmitted internally across the College network. In this case a risk assessment should be carried out to determine whether a cryptographic control is appropriate.

If sensitive data is to be transported in computer-readable storage media (such as magnetic tapes or floppy disks), it must be in encrypted form.

If encryption is used, the information protected with encryption must be transmitted over a different communication channel than the keys used to govern the encryption process.

The owner(s) of data protected via encryption must explicitly assign responsibility for the encryption key management to be used to protect this data.

### 7.10 *Software Installation, Configuration and Updates*

End users must ensure that they install and configure all software to a secure baseline standard. End users should ensure that they also install any updates or security patches that are available for the operating software application software or databases installed on devices connected to the College network or which are used to process or store College data.

Information Systems Services, Network Managers, system administrators, database administrators and application administrators must ensure that they install and configure all software in a secure manner and that they install all updates or security patches on operating systems, applications, databases and any other software, which they purchase, develop or administer.

Specific technical details on secure installation and configuration of operating systems and other software are available from the IT Security Officer or online at [www.tcd.ie/itsecurity](http://www.tcd.ie/itsecurity)

### 7.11 *Licensing*

Information Systems Services, Network Managers, database administrators and individuals are responsible for maintaining records of software licences for all software that they acquire.

Software that is acquired on a trial basis must be used in accordance with the vendor's copyright instructions.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	23 of 42



### 7.12 Copyright

Copyright stipulations governing vendor-supplied software must be observed at all times.

All software developed within the College is the property of the College and should not be copied or distributed without prior written authorisation.

### 7.13 Breach of Policy

Where software is found to be in breach of this policy and there is reason to believe that College information is at risk as a result, the IT Security Officer, Director of Information Systems Services, or Network Manager may have the software system/application withdrawn from live operation.

## 8 Data Backup Policy

Back-up procedures, ensuring that both data and software are regularly and securely backed-up, are essential to protect against the loss of that data and software and to facilitate a rapid recovery from any IT failure. This policy outlines guidelines for Trinity College staff and students on backing up College Data.

The data backup element of this policy applies to all Staff, students and third parties who use IT devices connected to the Trinity College network or who process or store information owned by Trinity College Dublin.

All users are responsible for arranging adequate data backup procedures for the data held on IT systems assigned to them

### 8.1 Best Practice Backup Procedures

All backups must conform to the following best practice procedures:

- All data, operating systems and utility files must be adequately and systematically backed up (Ensure this includes all patches, fixes and updates)
- Records of what is backed up and to where must be maintained
- Records of software licensing should be backed up.
- At least three generations of back-up data must be retained at any one time (grandfather/father/son)
- The backup media must be precisely labelled and accurate records must be maintained of back-ups done and to which back-up set they belong.
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	24 of 42





- Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency

### 8.2 *Responsibility for Data backup.*

Only critical systems are routinely backed up by Information Systems Services and Autonomous Network Managers in the current model. The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or by the College falls entirely to the User.

If you are responsible for a collection of data held either remotely on a server or on the hard disk of a computer, you should consult your Autonomous Network Manager or Information Systems Services about local back-up procedures. If you do not use the facilities provided by Information Systems Services or those of your own academic or administrative area you should put in place your own procedures.

### 8.3 *Legal Requirements*

Users when formulating a backup strategy should take the following legal implications into consideration:

- Where data held is personal data within the meaning of the Data Protection Act, there is a legal requirement to ensure that such back-ups are adequate for the purpose of protecting that data
- Depending on legal or other requirements, e.g. Financial Regulations, it may be necessary to retain essential business data for a number of years and for some archive copies to be permanently retained
- Depending on legal or other requirements, e.g. Data Protection Act, Software Licensing, it may be necessary to destroy all backup copies of data after a certain period or at the end of a contract.

### 8.4 *Desktop Backups*

The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or by the College falls entirely to the User.

All network users using personal workstations/laptops should ensure that their data is backed up using one or a combination of the following methods:

- Backing-up to a local device e.g. floppy disk, Zip Drive, CD-Rom.
- Copying critical data on a regular basis to a remote server that is properly backed up by the College.
- Backups should be scheduled regularly.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	25 of 42



- All users should backup their data before updating or upgrading software on their computer.

### 9 Disaster Recovery Policy

The disaster recovery procedures in this policy apply to Information Systems Services, Autonomous Networks and all College Users who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer.

#### 9.1 Published Disaster Recovery Plan/Procedures

- College must maintain a published and tested Disaster recovery plan as defined in section 9.3. This will be co-ordinated by the IT Security Officer.
- Information Systems Services and Autonomous Network managers must contribute details of data/systems owned by them and the plans procedures for disaster recovery annually.
- Information Systems Services and Autonomous Network managers must regularly schedule regular testing of the Disaster recovery plan or parts there of.

#### 9.2 User Responsibilities

All College users should make preparation for a disaster event in which IT equipment or data is destroyed. Users should:

- Ensure that they have backup up all important data stored on equipment owned by or assigned to them. Information Systems Services or an Autonomous Network manager can provide detailed advice on how best to achieve this.
- Note the procedures for procuring replacement hardware. This can be done by purchasing it from a suitable hardware vendor or by using spare capacity on a colleague's computer in other building/site.
- Maintain backup documentation regarding any licence keys that they may hold.

#### 9.3 Best Practice Disaster Recovery Procedures

A disaster recovery plan can be defined as the on-going process of planning developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of vital College functions in the event of an unscheduled interruption.

All disaster recovery plans must contain the following key elements:

- Critical Application Assessment
- Backup Procedures
- Recovery Procedures

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	26 of 42



- Implementation Procedures
- Test Procedures
- Plan Maintenance

### 10 Remote Access Policy

The purpose of this policy is to define standards for connecting to the Trinity College Network from a Computer or other device located outside of the College network. This policy is designed to minimise the potential exposure to the College from risks associated with remote access connections by ensuring only secure methods are used to connect to the College network.

This policy applies to all College Staff, students or Third parties with either a College owned or personally owned computer used to connect to the College network.

#### 10.1 *Permitted remote access connections*

Remote access connections to the College network may be made for College administrative or academic purposes only. These include but are not limited to:

- Approved use of network resources service by registered Staff and Students.
- Teleworking by registered College Staff.
- Network administration purposes by registered System Administration Staff.
- Administration of College Applications or Systems by approved Third parties.

#### 10.2 *Methods of Remote connection*

Information Systems Services and Autonomous network managers only may approve appropriate remote access technologies for use to access the College network.

College Users should apply to Information Systems Services or the Autonomous network managers for a list of currently approved methods.

Current preferred remote access technologies include but are not limited to:

- Approved College Virtual private network (VPN)
- Direct IP to IP PC Anywhere connection
- Direct SSH access

#### 10.3 *Non-standard remote access connections*

Organisations or individuals wishing to implement non-standard Remote Access must obtain prior approval from the [IT Security Officer](#).

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	27 of 42



### 10.4 *Protecting Remote Access Credentials*

All individuals are responsible for safeguarding the remote access credentials granted to them and making sure that unauthorised individuals do not use them. These credentials may consist of username and password combinations, digital certificates or other software or hardware.

### 10.5 *Username/Password Authentication*

Where Username/Password authentication is used the following apply:

- Where remote access authentication is facilitated using a username and password a strong password must be used as defined in section 5 of this policy document.
- At no time should any College staff member or student provide his or her username or password to any unauthorised third party.

### 10.6 *Remote Access Hosts*

All hosts that are used for remote access to the College networks must:

- Use the most up-to-date anti-virus software.
- Be protected by a College or private Firewall.
- Not be made available for use to unauthorised third parties.
- Be available for inspection by Information Systems Services or the Autonomous Network Manager/Administrator if requested.

### 10.7 *All Individuals/groups granted remote access connection Privileges*

It is the responsibility of all individuals/groups with remote access privileges to the College network to ensure that:

- Their remote access connection meets security standards as approved by the College.
- The connection is only used for approved purposes.
- The remote access credentials granted to them are held safely and not disclosed to unauthorised third parties.

### 10.8 *College Staff or Students providing remote access to Third parties*

College staff or students may only provide remote access to the College network to third parties with the express permission of Information System Services or the Network manager or Autonomous Network Manager.

College Staff providing remote access to third parties for any purpose must ensure that the method of remote access meets security standards as approved by the College.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	28 of 42



The Third party must be made aware of their responsibilities and provided with a copy of this policy document.

Details of the Third Party connection must be documented and submitted to the Autonomous Network Manager/Administrator or Information Systems Services.

### 10.9 *Third Parties*

It is the responsibility of all contractors, vendors and agents with remote access privileges to the College network to ensure that the remote access connection adheres to the Security Standards as defined in this policy.

All Third parties must comply with the security measures as outlined in section 11 of this policy document.

## 11 **Third Party Access**

The purpose of this policy is to define standards for all Third Parties seeking to access the College Network or any devices attached to the College Network. This policy is designed to minimise the potential exposure to the College from risks associated with Third Party Access.

### 11.1 *Scope*

This policy applies to all College Staff, students seeking to provide access to the College network or devices attached to the network to Third parties.

### 11.2 *Permitted Third Party Access*

Third party access to the College network may be made for College administrative or academic purposes only.

### 11.3 *Access Requests*

Requests to allow access to the College network or attached devices must meet the following criteria:

- Requests for third party access must be formally authorised in writing by the Information Systems Services or the relevant Autonomous Network Manager for the area prior to access being granted.
- The requester must agree to act as the sponsor for the Third Party and take responsibility for the actions of the Third Party when accessing the College network or attached devices.
- Where there is an approved need for third party access, security controls will be agreed and defined in a contract with the third party as detailed in section 11.4

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	29 of 42



- Access to Trinity College network facilities by third parties will not be provided until the appropriate measures have been implemented and a contract signed defining the terms for the connection.
- Third party access must be permitted only to the facilities, services and data, which are required to perform the specified tasks, as outlined to the IT appropriate Network Manager/Administrator in the original request for access.

### 11.4 Security Conditions in Third Party contracts

Third party access to College IT facilities must be based on a formal contract, which must address the following issues:

- A description of each facility, IT service or type of data to be made available must be included.
- Compliance with the published College Information Security Policy.
- Permitted access methods and the control and use of unique identifiers (User Ids) and passwords.
- A requirement to maintain a list of individuals authorised to use the service.
- A commitment such that all Third Party's granted access will inform the College in writing of staff changes that affect the integrity of security. This includes the rotation and resignation of employees so that the College can disable userids and remove / change passwords in order to secure its resources.
- Procedures regarding protection of College assets, including information.
- Responsibilities with respect to legislation including but not limited to the Data Protection Act
- The right of the College to monitor and revoke user activity.
- Responsibilities regarding hardware and software installation and maintenance.
- The right to audit contractual responsibilities.
- Restrictions on copying and disclosing information.
- Measures to ensure the return or destruction of information at the end of the contract.
- Any required physical protection measures.
- Measures to ensure protection against the spread of computer viruses.
- An acknowledgement that access to College systems and information will be granted for approved purposes only. The use of this access for personal use or gain is strictly prohibited.
- Arrangements for reporting and investigating security incidents.

### 11.5 Confidentiality

Where an individual has direct or indirect access to data or information owned by the College, this information must not be divulged or distributed to anyone. This is of particular concern when dealing with data that is registered with the Data Protection Commissioner.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	30 of 42



Documents which contain personal information including but not limited to names, addresses or telephone numbers, medical records, financial records of College staff or students must be carefully controlled and must not be released or disclosed to any unauthorised individuals or sources.

### 11.6 *Unique Authentication*

In order to ensure individual accountability on College Network devices and applications, all third parties granted access must be given a unique userid and password.

The third party will at all times be held responsible for any activities which occur on College networks and applications using this unique userid.

The Third Party is solely responsible for ensuring that any username and password that they are granted remains confidential and is not used by unauthorised individuals.

### 11.7 *Host Security*

When a Third Party is logged into the College network they should not leave the host they are logged onto unattended.

Workstations/laptops that are used to display College data should be located in such a way that confidential information is not displayed to unauthorised persons or the general public.

Up-to-date Virus checking software must be installed on any relevant devices that are being used to access the College Network or attached devices.

### 11.8 *Remote Access by Third Parties*

Where the type of access to be granted to the Network is from a remote device the third party must comply with the security measures as defined in 'section 10 of this policy.

## 12 **Incident Response and Misuse of IT Facilities Policy**

In the event of a security incident occurring, it is important that all College employees and students are aware of their responsibilities and the procedure by which incidents can be most effectively and efficiently brought to a satisfactory conclusion. The procedures as defined below are best practice within Trinity College.

Where investigation of a security incident indicates misuse of IT facilities approved disciplinary procedures will be implemented as defined in this policy.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	31 of 42



### 12.1 Incident Reporting

The types of incidents that must be reported include, but are not limited to:

- Incidents reported from Systems and Networks (system failures, unusual activity)
- Incidents that affect Senior Management (threats, gossip, leaks)
- Risk Management (unusual or suspicious behaviour noted in logs or activity reports)
- External sources (threats, customer queries, complaints, press)
- Incidents observed by network users (on local PC's or servers)
- All breaches of College Security Policy

### 12.2 Reporting an incident

All observed or suspected security incidents; weaknesses or threats to should be reported to an Autonomous Network Manager, Information systems Services or IT Security Officer.

In no instance should any user attempt to prove a suspected weakness as this could lead to a potential misuse of the system. Where users note that any software does not appear to be working correctly, i.e. according to specification, they should report the matter to the Helpdesk.

Where a user suspects that the malfunction is due to a malicious piece of software e.g. a computer virus, they should stop using the computer, note the symptoms and any messages appearing on the screen and report the matter to the Helpdesk.

### 12.3 Documentation

At all stages of the incident handling process adequate documentation must be maintained.

### 12.4 Disabling Accounts/Network Connections

Information Systems Services and Autonomous Network Managers may disable user accounts and/or network connections:

- Pending investigation of a security incident or where investigation of an incident
- To contain a confirmed security breach and prevent other College network devices from becoming affected by the incident.

### 12.5 Communication / Control

After validating that an incident has taken place Information System Services or the Autonomous Network Manager must escalate the incident to the IT Security Officer. The IT Security officer will contact any relevant staff and inform them of the incident. All persons briefed on the issue should be clear as to the sensitivity level and aware of the consequences of an information leak.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	32 of 42





### 12.6 *Obtaining Evidence*

It is vital that affected systems should be quickly identified and isolated. Information should be retrieved from these systems in the best available manner, with actions being taken by as few people as possible, preferably only the lead incident contact.

Incorrect gathering and handling of collected evidence may have serious consequences in the successful prosecution of an incident. Collected evidence therefore should be handled correctly so as to preserve integrity and all transfers should be documented and validated. Where possible collected data should immediately be stored on write-once media. Write-once media is defined as any media such as CD that once the data is written to it cannot be edited, amended or appended.

### 12.7 *Preserve Configuration*

The configuration and contents of all affected systems must be preserved to the greatest extent possible, so that the issues involved can be demonstrated at a later date. This may be covered by the method of obtaining evidence but may also involve manual backups of data. This must include all system configuration data as well as any scripts / data / files stored on the system.

### 12.8 *Query External Resources*

Where external resources are of use their outputs must always be recorded, preferably on a write-once media. This is particularly important for DNS lookups, whois / rwhois output, etc which may change at a later date. If personal contact is made with external agencies, details of all conversations / correspondence must be recorded in the relevant incident notes.

### 12.9 *Liaison with third parties*

If necessary the IT Security Officer must notify third-party partners of the incident, e.g. HEAnet. The decision to involve law enforcement should only be made by the senior management and details of all conversations / correspondence with the relevant law enforcement units should be recorded.

### 12.10 *Follow-up Actions*

The immediate incident team should draw up a change report detailing further changes required, including the priority and impact of each change. Approval for follow-up actions may be given by senior management or via normal change control process. The lead contact is responsible for tracking follow-up changes.

A detailed incident report must be prepared, including remedial action taken in the short and medium term, to help restore confidence in the systems affected.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	33 of 42



### 12.11 *Records of Security Incidents*

A sample report form to be used for documenting security incidents is included with this document. These records will be encrypted and stored securely for six months after which time information pertaining to individuals will be removed. The records will then be held in this anonymous format for a further two years for statistical purposes. The IT Security Officer will collate and analyse records of security incidents and will report to the College Board any trends which emerge and recommend any additional action which should be taken College wide to try to prevent their occurrence in the future.

## 13 **Misuse of College IT Facilities**

Where investigation of a security incident indicates misuse of IT facilities approved disciplinary procedures will be implemented as defined in this policy.

### 13.1 *Staff and Third Parties*

Where College Staff members or Third parties are found to have misused College IT facilities the Director of information Services, Network Manager or his nominated agent will inform the appropriate College authorities who will determine what further action should be taken.

### 13.2 *Students*

Where students are found to have misused College IT facilities the IT Security Officer, Network Manager or Administrator must inform the Junior Dean who will determine what further action should be taken.

### 13.3 *Student Disciplinary Offences*

Procedures for Dealing with Student Disciplinary Offences must be agreed periodically by the Junior Dean, the IT Security Officer, the Director of information Services and other Network Managers and System Administrators. These procedures should be documented and should agree summary punishment to be imposed on students breaking College regulations, which may comprise a fine or penalty. Attention must be paid to the magnitude and nature of misuse, which should be distinguished as below:

- Misuse - violation of the Conditions of Use of College IT facilities and associated Codes of Practice;
- Serious misuse - Serious violations requiring disciplinary hearing and/or legal proceedings;
- Criminal misuse - Violations necessitating legal proceedings. If the scale is of sufficient magnitude. In this event, the College may be obliged to inform the relevant state authorities,

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	34 of 42



### 14 Legal Compliance Guidelines

The College has an obligation to abide by all Irish legislation and relevant legislation of the European Community.

All users of the College Information Systems must ensure that they are fully aware of and understand any of the relevant legislation, which applies to IT systems or data, assigned to them.

This Guideline is not a full statement of the law, but is an indication of the issues to be complied with when processing information and disseminating it through the College Information Systems.

All users should be aware that Material stored electronically and available for access or use is considered to be a publication and is subject to laws applying to more traditional forms (e.g. Paper).

#### 14.1 *Relevant legislation*

Full copies of the acts outlined below are available from the College library and Information Systems Services.

- [Health and Safety Act, 1989](#)
- [Criminal Damages Act, 1991](#)
- [Freedom Of Information Act 1997](#)
- [Non-Fatal Offences Against the Person Act, 1997](#)
- [Child Trafficking and Pornography Act, 1998](#)
- [Intellectual Property \(Miscellaneous Provisions\) Act 1998](#)
- [Data Protection Act, 1988](#)
- [Electronic Commerce Act, 2000](#)
- [Copyright and Related Rights Act, 2000](#)
- [eCommerce Directive \(2000/31/EC\)](#)
- [European Communities \(Data Protection\) Regulations, 2001](#)
- [European Communities \(Data Protection and Privacy in Telecommunications\) Regulations 2002](#)
- [Data Protection EU Directive 95/46/EC](#)
- [Data Protection \(Amendment\) Act 2003](#)
- [Regulations entitled European Communities \(Directive 2000/31/EC\) Regulations 2003 \(S.I. No. 68 of 2003\)](#)
- [HEAnet Acceptable Use Policy](#)

#### 14.2 *Confidentiality*

Users have a duty of care to protect the confidentiality of any information, which they might access though the College network in the course of legitimate employment activities or through academic studies.

#### 14.3 *Unauthorised Access Attempts*

Attempts by users to access, alter or erase data that they have not been authorised to access by

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	35 of 42



the data owner, or attempts to use any username, which is not authorised to the user, are prohibited.

Such attempts may be in breach of the Criminal Damages Act (1991).

### 14.4 *HEANET Acceptable Use Policy*

Users must not use or attempt to use any network or networked service accessed from the College for unauthorised purposes and, in particular, the HEANET network which is subject to the HEANET Acceptable Use Policy. ("HEANET" is the name given to the collection of networking services and facilities, which support the communication requirements of the Irish education and research community). Unacceptable use, in addition to use, which contravenes national legislation, also includes the transmission of unsolicited commercial or advertising material either to other user organisations or to organisations connected to other networks.

### 14.5 *Copyright, Intellectual Property and Patents.*

Under the Copyright and related acts, 2000 it is unlawful to take an unauthorised copy of someone else's work. A person holds the copyright in that work if it is the product of their intellectual activity and hence is their intellectual property, although if that work is done as part of your employment the intellectual property and hence the copyright, is owned by the College. This applies to a large amount of material on the Web including buttons, icons and text. Also, unless otherwise stated, all software found on the network is protected by this Act and should not be copied unless it is specifically stated to be in the public domain.

Do not use someone else's work unless,

- You have that person's permission in writing
- You are sure that the material is not protected by copyright.

Usage includes storing and displaying material electronically. Also, publishing your own or somebody else's ideas or material may jeopardise future patent applications.

### 14.6 *Libel*

Facts, which concern individuals or organisations, must be accurate and verifiable. Views or opinions must not portray their subjects in any way, which would damage their reputation. If publishing research data, you should be aware that organisations and individuals might be identifiable. Libel is a civil offence and incurs financial penalties.

### 14.7 *Protection of Minors*

The Internet is becoming more accessible to minors through computers in homes and schools.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	36 of 42



Material must not be published which might lead to injury or damage to minors. This includes material that is pornographic or excessively violent. Users should be aware that some legitimate research documents might include material of a medical nature, which is unsuitable for minors who must, therefore, be protected from unauthorised viewing.

### 14.8 *Sexually Explicit Material*

The retention or display of pornographic or sexually explicit material is forbidden by the College, as is the enabling of links to sites containing such material. This is irrespective of whether that material is legal in this country or any other.

### 14.9 *E-commerce Act*

The Electronic Commerce Act 2000 implements the EU Electronic Signatures Directive 1999/93/EC and it was seen as a necessary step in the development of E-Commerce.

The main principle of the Act is that electronic signatures, electronic contracts or electronic documents have the same legal recognition as written signatures, contracts or documents in relation to commercial and non-commercial transactions.

The Act introduces for the first time in Ireland the concept of advanced electronic signature.

Where information is required in "writing" in any other Act or instrument under an Act, this requirement can include an electronic form.

All electronic contracts within the State are subject to all existing consumer legislation.

### 14.10 *Unsolicited Commercial Emails*

(S.I. No. 68 of 2003) effective as of 24/03/03 transposes into Irish law the essential requirements of EU Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market.

In particular the Regulations require persons sending unsolicited commercial email to ensure that these are clearly identifiable on receipt.

All College network users should seek advise from the [IT Security Officer](#) before sending unsolicited commercial email. Failure to comply with this provision is an offence prosecutable by the Director of Consumer Affairs or the Data Protection Commissioner.

### 14.11 *Freedom of Information*

The College became a prescribed 'public body' subject to the terms of the Freedom of Information

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	37 of 42



Act, 1997, from 1 October 2001.

The Act established three new statutory rights:

- (a) A legal right for each person to access records held by public bodies;
- (b) A legal right for each person to have records relating to him/herself held by public bodies amended where they are incomplete, incorrect or misleading;
- (c) A legal right to obtain reasons for decisions affecting oneself made by public bodies.

Records are defined very broadly by the Act and include anything in which information is held manually, mechanically or electronically. This would include, for example, electronic data, electronic files or e-mails.

Further information and advice about the Act and its implications are available from the Freedom of Information Officer who may be contacted *by post* to The Secretary's Office, West Theatre, College, *by e-mail* to [foi@tcd.ie](mailto:foi@tcd.ie) or *by telephone* to (01) 608 2154, or from the College's Freedom of Information website [www.tcd.ie/foi/](http://www.tcd.ie/foi/). All requests to the College made under the Act should be in writing and addressed to the Freedom of Information Officer, who can advise on how to submit a request.

### 14.12 Data Protection Act

Trinity College Dublin keeps information about its staff and students to allow it to perform key tasks. Personal data is processed so that customer expectations can be met, legal obligations fulfilled, and staff recruited and paid. To comply with data protection law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must follow the Data Protection Principles, which are set out in the Data Protection Act 1988 and further expanded in the EU directive 95/46/EC.

The College's registration/notification under the Act and details of personal data held by the College on an individual may be seen by application to the College's Data Protection Officer.

The processing of personal data, in the College must to be registered with the College Data Protection coordinator.

Further information on the data protection Act is available in the College published Data Protection Policy' available at [http://www.tcd.ie/info/policies/data\\_protection.php](http://www.tcd.ie/info/policies/data_protection.php)

For general information on Data Protection please consult the Data Protection Commissioner web site on [www.dataprivacy.ie](http://www.dataprivacy.ie)

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	38 of 42



### 14.13 *College Compliance with Data Protection Act*

In order to comply with the Data Protection Act Trinity College Dublin must:

- Hold the minimum personal data necessary to enable it to perform its functions,
- Ensure that data is erased once the purpose for which it was obtained has been achieved. unless there are overriding legal or regulatory reasons why this should not be the case. Such reasons should be documented.
- Ensure that personal data is accurate and up-to-date, and that inaccuracies are corrected without undue delay.
- Ensure that personal data is treated as confidential. Sources and disclosures of personal data must be in accordance with the College's registration under Irish data protection legislation or other applicable rules.
- Provide to any individual who asks, a reply stating whether or not the College holds personal data about that individual. A written copy, in clear language, of the current data held will be given. A fee may be charged for this service.
- Compliance with this Data Protection statement of practice is the responsibility of all members of the College. Any deliberate breach of this Data Protection statement of practice will be dealt with under Colleges disciplinary procedures, criminal sanctions can also apply. Any questions or concerns about the interpretation or operation of this statement of practice should be taken up with the Data Protection Co-ordinator.

### 14.14 *Subject Access Request under Data protection legislation*

Staff and students of the College have the right to access any personal data that the College is holding about them either on computer or in certain manual files subject to certain conditions. Any person who wishes to exercise this right should contact the Data Protection Co-ordinator. A charge may be made on each occasion that access is requested.

The College must first confirm the identity of the person making the subject access request. This may involve the subject providing sufficient information to accurately identify him or herself. Once the identity is established, the College must provide, subject to certain legal constraints and third party rights:

- A copy of all information held on the data subject
- A description of why the information is held
- The names of anyone to whom it may be given or shown

The College will ensure that information is provided within 40 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the access request.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	39 of 42



The Data Protection Coordinator will ensure that anybody wanting to make enquiries about handling personal data knows what to do and that any such queries are promptly and courteously dealt with.

### 14.15 *Data Protection Exclusion Rules*

Information about a data subject, which would be likely to affect:

- The way crime is detected or prevented
- Catching or prosecuting offenders
- The assessment of taxes or duty need not be included in the reply. There are also specific rules on information, which reveals the name of a third party (i.e. any other person mentioned in the data such as, for example, the name of a spouse or dependent).

### 14.16 *Data Protection Subject Consent – Staff*

The College will publish information from time to time about individual staff and student members (e.g. internal extension number, email address etc), which is necessary for the efficient running of the College. Any individual who has good reason for wishing such information to remain confidential should contact the designated Data Protection Co-ordinator.

It may be necessary to process information about a person's health, criminal convictions, race, gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies such as Equal Opportunities. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff will be asked to give express consent for the College to do this. Offers of employment may be withdrawn if an individual refuses to consent to this, without good reason.

### 14.17 *Data Protection - Retention of Data*

The College will need to keep information about staff for long periods of time. In general all information will be kept for three years after a member of staff leaves the College. Some information will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding employment, and information required for job references. A full list of information with retention times is available from the Data Protection Co-ordinator.

### 14.18 *Data Protection - Security*

Under this Data Protection statement of practice, security measures apply not only to the security of computer hardware and storage media, such as computer discs, but also to supporting source documents, manual records, printouts and oral disclosure. Security measures are applicable

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	40 of 42





throughout the use and processing of personal data, including the handling, transmission, disclosure and disposal of documents containing personal data.

### 14.19 Data Protection - Processing Data Off-Site

Vigilance is required when personal data, which has been gained by virtue of employment at the College, is processed off site. This is only allowable if: the personal data is used or processed in accordance with the duties of the member of staff and for no other purpose the processing activities are in accordance with the terms of the College's registration with the Data Protection Commissioner security regulations are followed

### 14.20 Data Protection- Future Developments

Although the European directive 95/46/EC has not been implemented by national legislation in Ireland it will become law. The College, through the implementation of this statement of practice, will comply with its provisions as far as these can be anticipated. The Minister for Justice, Equality & Law Reform recently introduced new regulations, which will bring into force some parts of the EU Data Protection Directive, with effect from 1 April 2002. The new rules relate mainly to the transfer of personal data to countries outside of the European Economic Area. Contact should be made with the Data Protection Co-ordinator if personal data is being transferred outside of the European Economic Area (which comprises of EU Member States and EFTA countries excluding Switzerland).

### 14.21 Data Protection - User compliance

- Users must be aware of and comply with this policy.
- Users must register a new database when they download personal data for use.
- Ensure that any of their own personal data provided to the College is accurate and up-to-date; inform the College of change of address or other circumstances; check and, where required, correct the personal data that the College may send out to them from time to time.
- Remember that personal data can be contained in e-mails that can easily be forwarded to other parties. Users should assume that anyone mentioned in e-mail will see it or hear about it – or he/she may, under data protection or other law, be entitled to see it.
- Ensure that third parties are aware of this statement of practice and that they take appropriate measures to protect any personal data. Non-disclosures agreements should form part of every contract if they are subject to personal data.
- Ensure that personal data is accurate, factual and objective. Avoid subjective opinion about people or other organisations.
- Work on the basis that access will be audited for compliance with the law and internal policies.
- Hold personal data securely e.g. using locked cabinets and desk drawers.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	41 of 42



### 14.22 Breach of Data Protection Act

Users must not breach the Data protection act in the following way:

- By sending e-mail to external e-mail addresses for exchanging personal data without consulting the IT Security Officer about additional protection measures. This is two way, as third parties may e-mail personal data to you
- By disclosing personal data orally or in writing, accidentally or otherwise to any unauthorised third party.

Author	IT Security Officer	Information Security Supporting Policies.doc
Last Revision Date	08/02/2007	42 of 42