IT Security Policy

Owner:	Director of Information and Learning Technologies
Issue Date:	May 2017
Review Date:	May 2018

This document is prepared and managed by IT Services on behalf of Colchester Institute and is intended for users and system administrators and relates to the IT security standards maintained across all IT systems within the College.

The College's Views on Information Security

The College is committed to ensuring the integrity of computer based information required for its operation and compliance with relevant legislation covering this area. Most notably this includes compliance with the Data Protection Act 1998. To maintain this integrity in what can be regarded a transient medium, the College believes that it is essential to establish and conform to clearly defined standards of operation in relation to computer based information. To assist with this the College has developed this IT Security Policy, which will be reviewed and updated annually.

The College also aims to make users aware of this policy and also of other relevant standard practice and legislation, and how to achieve compliance with them.

Policy Statement on Information Security

1 The College seeks to ensure that all computer based corporate information generated and used within it is accurate and appropriately available.

2 All sections of the College controlling access to computer-based information will conform to the IT Security Policy.

3 All data connections to external bodies will be validated to conform to the IT Security Policy.

Principles of Implementation

Scope

The IT Security Policy covers all internal College systems and connections to wider networks. All new systems must have their security controls agreed by the IT Services Manager, or nominee.

Conditions

- All systems within the College and connections to outside bodies must conform to this Policy. IT Services will ensure that the Policy is put into practice.
- The College reserves the right to isolate any system or network which represents a potential or actual breach of security.
- The College reserves the right to monitor information sent over its networks.

Access Control

- All systems, except those designed for public open access, are required, at their point of entry, to have an auditable sign-on procedure with a unique, traceable Identifier and Password.
- All backend server facilities remotely accessible must have approval from IT Services.
- All external access will be audited to ensure traceability and responsibility.
- Access and connection to selected wider networks will be restricted to authorised Users only.
- The College reserves the right to deny systems access to users.

Security Breach Handling
IT Services, or a party designated by it, will be responsible for and/or deal with:

- All incidents that affect, or could affect information security.
- The monitoring of security breaches.

Data Protection
Users who input data on to the College's networks and systems are responsible for ensuring that they comply with the requirements of the Data Protection Act 1998. This is encapsulated in the Colleges Data Protection Policy and Retention of Records Policy. Other legislation to consider:

- Computer Misuse Act 1990 Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003 Terrorism Act 2006 s3
- Police and Justice Act s35-38

Copyright Software
Copyrighted and licensed software must not be duplicated, removed or added by Users unless it is explicitly stated that they may do so.

College Information
The term 'College information' as used in this document is generally defined as information relating to the running of the College. This may be personal information related to students, staff, external customers and contractors, and includes documents and files containing corporate commercial and confidential matters, and also information the College's business and research partners have shared with the College.

Responsibility

- Responsibility for compliance with the policy is delegated to CMG and business managers within their respective Faculties and Services.
- Responsibility for the security and integrity of the College data infrastructure lies with IT Services Manager or at certain formally agreed locations, a party designated by it.
- Departments and services with special facilities are responsible for those facilities. Facility managers are obliged to address any matter that IT Services identifies as a possible security threat.
- Individuals are responsible for their own actions and usage of their assigned Personal Identifier.
- Individuals are responsible for ensuring that they comply with all the requirements of the ILT Code of Conduct.

This document and computer network security standards as implemented at the College must be complied with by all College computer systems. The relevant areas are covered in sections for ease of reference as follows.

The words 'computer system(s)' are used in this document to encompass all campus networks, servers, workstations, virtual terminals and network access

devices.

All departments and services with locally administered computer systems and networks are required to adhere to the security requirements of this document.

All departments and services with connection to the Internet are required to adhere to the security requirements of this document.

All User queries and notifications relating to the contents of this document should be addressed to the IT Services Manager.

CONTENTS

1. ACCESS CONTROLS

General

1.1 The computer system will have appropriate access controls. These controls will be defined for access to entire computer systems, specific data files, software applications, email and other resources. Access controls can be specific to individual Users or to groups of Users. Users will only be permitted access to those files and system resources they need to perform their job functions. In a computer system environment, considerations will include:

- Identification of the User to the computer system by Account Name and Password
- Access to *required* Files and Folders
- Account Restrictions
- Time Restrictions (set times of day between which the account may be used)
- Access to Databases and associated Applications Software
- Other Privileges

Access controls on User Accounts

1.2.1 Individual Users will each be given a personal account for which they are held responsible.

1.2.2 Group accounts will be permitted where necessary for specific purposes, but they will be suitably limited in function. By definition, a group account is used by more than one authorised person, which makes it harder to determine who performed any specific action. Users of any group account must understand their responsibilities for its security and only use it in the manner agreed.
A group account may be withdrawn if, in the judgment of IT Services, the account or the manner in which it is used is thought to present a security risk.

1.2.3 User accounts will be reviewed on a regular basis, and any accounts that are no longer required will be removed. See the section, User Identification and Authentication for further details.

1.2.4 A User should not log in to more than one session at a time except where absolutely necessary for specific work to be performed.

1.2.5 Users will be given an appropriate restricted file store space for their work purposes. Users will be required to tidy this file store space on a regular basis by deleting files no longer current. Refer to retention of records policy.

Access to Files

1.3.1 User access to files will be granted according to individual or department need. By default, access will be denied unless it is shown to be required.

1.3.2 Access to files containing confidential or sensitive information will be restricted. Only those Users needing the information shall be given access to it.

Access to Databases and their Associated Applications

1.4.1 There will be access controls on databases and associated software in line with current best practice as recommended by the relevant software vendors.

System Administration

1.5.1 Sensitive system commands and software will be restricted to system administrators and security personnel.

1.5.2 Accounts with enhanced file access rights or with high level access to computer systems will be used only when necessary to perform tasks requiring such access. Excessive and unnecessary use will expose the computer system to increased risk of virus infection and damage to the file system and software.

Permitted Use

1.6.1 All Users must be acquainted with and required to conform to current IT Facilities Rules as administered by IT Services. These detail acceptable usage standards within the College. All users of IT facilities must adhere to the rules set out in this IT Security Policy and the Rules governing the use of the IT facilities.

1.6.2 Access to information held on a User's account other than by the User can only be performed by the IT Services Manager, nominee, or by other delegated authority of the IT Services Manager.

1.6.3 Access to a staff member's Colchester Institute IT account or Colchester Institute email system will be made available to the staff member's line management, Human Resources or IT personnel, where there is good reason to do so, for example due to staff absence or to facilitate an investigation. Access will be granted where permission has been expressed in writing by a member of the College Management Group. On receipt of the authorisation, the IT Service Desk will follow an appropriate protocol that will determine whether full access really is needed, as in some cases the ITSD may be able to resolve the matter (eg by amending an out of office message or placing a forward on emails). Where appropriate the IT Service Desk job process will be used to inform the individual staff member of access that has been authorised.

2. AUDIT CONSIDERATIONS

Computer logs are records of past events on a computer system. Logs can accumulate a great deal of information over time, which can be very useful to investigators piecing together what took place during a security incident. Logs can be audited to help spot an *attempt* to breach system security, and can also be useful as evidence in a misuse enquiry.

Types of information recorded in computer logs include (but are not limited to)

- The dates and times of account logins and logouts
- Internet use and email traffic
- The behaviour and health of the computer system itself.

2.1 Use of computer accounts and Internet usage will be logged and recorded as required by current legislation.

2.2 Software logs will be enabled as appropriate to comply with license conditions.

2.3 Where appropriate, computer systems will always log User activity to provide an audit trail so that actions can be traced back to individuals e.g. when there is a case of suspected misuse.

2.4 Attempts to breach security will be investigated immediately. If an attempted breach or an actual breach impacts on any corporate computer systems, staff discovering the problem must immediately notify IT Service Desk.

2.5 System administrators will regularly review computer logs to detect attempts to breach system security.

2.6 Where checks of computer logs raise suspicions of attacks on the computer system, actual security breaches or other irregularities, system administrators will promptly investigate such concerns.

2.7 The corporate computer system will maintain correct time by automated reference to a nationally recognised time source. All corporate systems will synchronise their clocks according to this time.

2.8 The administrators of non-corporate systems will be responsible for ensuring the time on those systems remains consistent with the time on the corporate systems. IT Services is registered with JANET for access to its NTP service, and administrators should make use of this where possible.

2.9 The administrators of non-corporate systems will be responsible for retention of usage logs on those systems for periods prescribed by IT Services in line with national best practice and legal guidelines.

3. BACKUP AND RECOVERY

3.1 Backup of server files will be automated and will be scheduled on a regular basis.

3.2 The technologies for performing data backups and the schedules used must meet the business requirements of the College.

3.3 Backup sets will be tested regularly to ensure the backup system is reliable and data can be recovered in the event of a disaster recovery scenario.

3.4 Several generations of backup files will be maintained.

3.6 At least one backup copy will be available on-site in case recovery is necessary.

3.7 At least one other copy will be stored at an off-site location in case of a fire or some other contingency at the main site.

3.8 All College information and User files will be stored on the College's network. Users must be aware that College information and User files are not stored on their workstations. The system administrators do not (and cannot) back up files held on workstations, and therefore it is vital that Users store files on the network to ensure backups can be taken.

3.9 Any Users with authorisation to use local hard disk (fixed or mobile) storage

- are responsible for their own backups
- will not use this private space for College information

3.10 Users are advised not use "cloud" based services for backups or for the storage of College information. It is also not permitted to use such services for the transfer of College information between portable computing devices and the College's network. Such "cloud" based storage services have been known to operate security and Data Protection regimes which are currently not compatible with the College's own security and data protection requirements. As use of these services is considered a threat to confidentiality, their use with College information is not permitted.
For further advice, contact IT Service Desk on extension 2222 or by email at itservicedesk@colchester.ac.uk

4. DATA CONFIDENTIALITY CONSIDERATIONS

Refer also to the College Data Protection Policy.

Any exceptions to these general rules must be by agreement with the IT Services Manager, or nominee. In such cases, Users must comply with security protection measures that may be prescribed.

General

4.1.1 Where data has been identified as personal, confidential or sensitive, precautions will be in place to restrict access to the data to those individuals who need it to do their job.

4.1.2 Users must apply the same confidentiality considerations to paper copies of personal, confidential or sensitive information.

4.1.3 In line with the guidance stated in the section 'Use of Computers', College information including corporate, personal, confidential, or otherwise sensitive information will be stored only on the network in the appropriate shared areas or the database systems.

4.1.4 If College information is to be transported on USB memory devices

- The USB device used **must** be an encrypted/protected type approved by IT Services.
- Non-encrypted USB memory **must not** be used to hold College information.
- The storage **must** be *temporary* and only for transportation and transfers.
- The User **must** take great care to ensure current files are not overwritten with old versions, and that incorrect or out of date information is not imported for processing.

4.1.5 The use of e-mail for the transfer of personal, confidential or sensitive information is not recommended. Where there is no better alternative, its use is acceptable on condition that the User

1) takes proper care to address email messages correctly
2) considers
   - The sensitivity or confidentiality of the information
   - What damage or distress could be caused to individuals if the information was delivered to the wrong place or was involved in some other security breach
   - The effect a security breach involving the information could have on the College
     a) In cost
     b) To our reputation
     c) To the trust of our customers and clients

If the answer to the above assessment indicates negligible risk then encryption may not be required. If the harm caused would be considerable then the user must follow the related guidance on the use of encryption.

For specific queries related to sensitivity of information and Data Protection, please refer to the College's Data Protection Policy.. Refer also to the guidance notes on Managing Email for more information.

Protection of Offices, Workstations and Printouts

4.2 Users must ensure that:

4.2.1 Workstations, printers and other output devices are not left unattended or in other circumstances where it may be possible for unauthorised parties to view or access personal information, confidential or other sensitive information.

4.2.2 Workstations are shut down and logged out overnight and when the user is otherwise absent for a long period of time.

4.2.3 Where technically possible, workstations are locked when temporarily unattended. (Windows key + L key)

4.2.4 Offices are kept locked to keep unauthorised parties away from computer equipment when staff are not in attendance.

4.2.5 Output containing personal, confidential or sensitive information is held securely e.g. under lock and key.

4.2.6 Printouts containing personal information, confidential or sensitive information are treated as confidential waste when disposed of and are shredded instead of being thrown out as general waste paper.

Safe Disposal of Equipment Used for Data Storage

4.3.1 All sensitive information is removed from hard drives in file servers before the equipment is turned over to maintenance personnel or the maintenance personnel follow the data erasure procedures agreed in their contract.

4.3.2 Departments and services who have been authorised to store College information on any equipment other than the network must adhere to the CI *Data Protection Policy*. Users must be aware that non-observance of this guidance may in some cases contravene Data Protection legislation, particularly where equipment is sold off or donated to another individual, school, or service.

4.3.3 Departments and services who have been authorised to store College information on any non-corporate hard drives are responsible for ensuring that the equipment is not sold on or donated without being properly erased.

Data sharing and Transfers

4.4.1 If there is no better option than electronic mail for the transmission of personal, confidential or sensitive information, the User **must follow the guidance in the table below regarding when encryption should be used and carefully ensure the message is correctly addressed**. The possibility of misaddressing could mean the information is delivered into the wrong hands, and it is the responsibility of the User to guard against any such unwanted disclosures and comply with the Data Protection Act 1998.

4.4.2 If using electronic mail for the transmission of personal, confidential, or sensitive information, the User must follow the current guidance on whether to use encryption. The method of encryption is prescribed by IT Services.

Type of Scenario	Is Encryption Required?
Personal information about **1** person sent to **internal** email address	No, but the User **must** take care to use the correct email address
Personal information about **1** person sent to **external** email address (any address *outside* the College)	The user **must** follow the guidance in paragraph 4.1.5 on assessing the sensitivity of the information. If the risk is negligible then there is no requirement for encryption, but the User **must** keep information to the minimum required and **must** take care to use the correct email address. If the information to be transmitted is highly sensitive then the User **must** make effort to arrange with the recipient for the recommended encryption to be used.
Personal information about **many** people sent to **internal** email address	Encryption is advised. In any case, the User **must** take care to use the correct email address.
Personal information about **many** people sent to **external** email address (any address *outside* the College)	The User **must** make effort to arrange with the recipient for the recommended encryption to be used. This could include upload to a protected third party site

As evidence of good practice, Users are advised to retain email messages from information recipients discussing whether the recommended encryption can be used.
Queries concerning the above table should be addressed to IT Services on extension 2222 or by email at itservicedesk@colchester.ac.uk .

4.4.3 Users must conform to personal and corporate privacy concerns in any data transfers including e-mail.

Please refer also to the College's *Data Protection Policy*, the requirements of the European Directive 2002/58/EC, and also the Privacy and Electronic Communications (EC Directive) Regulations 2003

4.4.3 Faculties, departments and schools must not disclose or share personal data with external bodies for the purposes of marketing or provision of services without the data subjects first being given the choice to opt out. The IT Services Manager, or nominee, must approve any agreements to share information held on corporate electronic systems.

4.4.4 Users must not send or otherwise disclose, to external parties, photographic images of other individuals obtained from the College's systems.

External Mail Systems (and "Cloud" Storage Services)

4.5.1 Users are reminded that electronic mail systems hosted by external providers are outside the control of the College. Such systems must not be used for official College business or for the storage of corporate, personal, confidential or otherwise sensitive information.

4.5.2 Users are not permitted to use personal "cloud" based file storage/sharing services for the storage of College information or for data transfers between colleagues unless specifically authorized by the IT Services Manager. Such systems and their security controls are outside the control of the College, and as they sometimes operate security and Data Protection regimes which are not compatible with the College's own security and data protection requirements. As use these services is considered a threat to privacy and data confidentiality, their use with College information is not permitted.

Manual Records

4.6.1 Users must handle information held on manual records according to the relevant procedures.

Credit Card Records

4.7.1 Users should never store or transmit sensitive Credit Card data including but not limited to the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN).

4.7.2 User should refer to and adhere to the College's PDQ Information Security Policy (PCI DSS SAQ B) for further guidance.

5. DISASTER PREVENTION

Precautions

Disaster Prevention is an area concerned with preventing a disaster from ever happening or at least minimising its effects if one does occur. The following precautions must be implemented by system administrators to mitigate disaster impact.

5.1.1 Data backup systems must be fully implemented, be tested regularly and be available for use if files need to be restored.

5.1.2 The servers and networking equipment will be located in secure locked rooms to which access is restricted to authorised persons.

5.1.3 Critical services will, where possible, be duplicated for resilience.

5.1.4 Critical equipment must be covered by Uninterruptible Power Supplies to protect against power supply problems.

5.1.5 Appropriate fire detection/prevention systems will be installed in the corporate computer rooms.

5.1.6 College Security Personnel will respond to activations of intruder alarms and fire detection/prevention systems relating to the corporate computer room. Where appropriate the emergency services will automatically be notified of activations for the fastest response.

Business Continuity Planning

5.2.1 A Business Contingency Plan has been formulated to ensure key personnel and resources are available to expedite recovery when a disaster does occur.

5.2.2 The Business Contingency Plan must cover all the essential and critical activities of the College.

5.2.3 Key personnel must be made aware of the Business Continuity Plan, how it is to be executed, and understand their own respective roles.

5.2.4 The Business Continuity Plan must be reviewed, kept up to date with technical developments and the changing needs of the College, and periodically tested to ensure the response options remain appropriate and adequate.

6. DOCUMENTATION

Computer system security controls must be adequately documented to allow for effective security and use of the network.

6.1 IT Services will prepare appropriate documentation for corporate systems.

6.2 Administrators of non-corporate systems will prepare appropriate documentation for those systems.

7. HARDWARE FAILURE RECOVERY

7.1 Hardware will fail occasionally. IT Services will assess how critical each corporate system is to the operation of the College. Appropriate arrangements shall be made for hardware maintenance (or replacement) to allow recovery within acceptable and realistic time scales.

7.2 Where possible, critical computer systems will be 'fault tolerant'; they will be designed so that there is no single point of failure. In other words, a failure in one part of the system shall not cause a total failure. Where possible, parts of the system shall be duplicated. This way, a failure in one part can be tolerated because other parts performing the same function share the workload and are still operating. Where this is not economically or technically possible, appropriate maintenance procedures must be in place to maximise reliability of the service.

8. MEDIA PROTECTION

8.1 Computer media will be stored and handled according to manufacturer's instructions and subject to the Colleges Retention of Records policy.

9. NETWORK MANAGEMENT/PROTECTION CONTROLS

Protection for the External Network Link

9.1.1 The external network link is managed by IT Services to provide security, control and auditing of usage.

9.1.2 Any computer systems using the external network link must have approval from IT Services to do so. The administrators of such systems must ensure compliance with the security requirements of this document.

9.1.3 Any broadband/ISDN access must not be connected to the main College networks but must connect through an IT Services managed or authorised firewall to avoid compromising security, or be completely stand alone.

Firewalling for Networks belonging to Colchester Institute and Services

9.2.1 All non-corporate networks belonging to departments and services must be authorised by IT Services.

9.2.2 It is the responsibility of the individual department or service to ensure that its non-corporate network is not the source of any unsolicited intrusion (whether malicious or not) to the corporate network or the facilities of any other member of the JANET community.

9.2.3 Failure on the part of the individual department or service to adequately police its non-corporate network will result in that network being immediately isolated by disconnection until such time as IT Services is satisfied that there is no longer any risk.

9.2.4 Each department or service with a non-corporate network must use the corporate, IT Services managed firewall to protect it from unsolicited external approaches.

User Authorisation

9.3.1 The College will ensure that all computer system users are formally authorised to use the network and an audit trail of authorisation is maintained. Users will be removed when their employment ceases at the College.

9.3.2 Students are authorised by the Student Registry as being fee paid students of the College. Refer to section 14 for details on account expiry.

9.3.3 Staff are authorised by Human Resources and their line manager with sensitive data access being specifically requested.

9.3.4 External Users are authorised by IT Services and may be given access to computer systems where appropriate.

Hardware Authorisation

9.4.1 IT Services will maintain an inventory of authorised network equipment including network components, servers and workstations. Unauthorised hardware will be removed.

Controls on Physical Access to Computer Equipment

9.5.1 Physical access to the servers and related components will be limited to authorised personnel.

9.5.2 The servers, backup facilities, UPS, network hubs, etc. will be installed in locked areas which are only normally accessible to the computer system administrators and relevant technical support staff.

9.5.3 Rooms used to house server and other sensitive system equipment will be kept locked and access to them restricted and monitored.

9.5.4 Where workstations are located in public areas or areas that can be accessed by the public or students, consideration will be given to securing workstations and printers to desks and installing CCTV monitoring equipment.

Prohibition of Non-Standard Hardware and Software

9.6.1 Non-standard hardware and software is defined as any equipment that does not have an IT Services developed and maintained operating system.

9.6.2 The corporate network is defined as any and all infrastructure intended to support the corporate IT requirements.

9.6.3 All devices connected to the corporate network are to be standard hardware managed by IT Services. Any non-standard hardware and software must be hosted on an existing non- corporate network behind firewall protection.

9.6.4 Any exception to the above is by the prior express permission from the IT Services Manager, or nominee. This is subject to a security risk assessment, which must be made by suitably qualified IT Services staff.

The IT Services Manager, or nominee, may refuse.
Reasons for refusal are various, including but not limited to the following

- In the judgment of IT Services, the equipment might in any way interfere with, or be a risk to, the correct functioning of the corporate network or any approved systems,
- The equipment has inadequate protection against infection by malicious software.
- The equipment is not properly secured against unauthorised access and misuse.

Wireless Keyboards

9.7.1 Wireless (including Bluetooth) input devices constitute a potential risk to information security as there is little or no privacy on the wireless link. Anyone within close proximity (30 metres) may monitor keystrokes and mouse movements. If there is a similarly equipped PC within range there are circumstances under which control of one PC may transfer to the other keyboard or mouse. It is for this reason that they are not approved for administrative use on the College network.

9.7.2 Similar consideration should be given to the use of wireless input devices in the home environment. Individuals using such devices on personal PC equipment whilst remotely accessing corporate systems and/or data must be aware of the risks and take appropriate measures to protect against possible breaches of security.

Workstation Client Software Protection

9.8.1 IT Services will deploy security related software patches and updates to the corporate computer systems.

9.8.2 The administrators of non-corporate systems will be responsible for the deployment of the relevant security related patches for those systems.

Protection of Web-based Services

9.9.1 Certain web-based services, for example access to College databases containing personal or confidential information, will have extra protection against eavesdropping on the Internet. SSL (Secure Sockets Layer) will be used to establish a secure connection between the client and server for transmission of information in encrypted form.

Procedural Requirements

9.10.1 IT Services will remove all sensitive information from all file server based on-line storage devices before the equipment is turned over to maintenance personnel or or the maintenance personnel follow the data erasure procedures agreed in their contract.

9.10.2 All Users and administrators will be made aware that they will report all cases of security violations to their supervisor and the system administrator. Potential or actual violations of security of corporate systems will be reported to IT Service Desk on extension 2222.

Audit Trails

9.11.1 IT Services will maintain a record of usage by User and workstation to aid efficient resource planning, incident response, and to provide an audit trail for misuse investigations.

Risk Analysis

9.12.1 Responsibility for conducting periodic risk analysis and security assessments will be formally assigned. The owner of the computer system is responsible for assigning responsibility for periodic risk analysis and security assessments of the computer systems.

9.12.2 Risk analysis and security assessments will be conducted during the system design stages and at any other times when changes are made to the system design and/or components. Such analysis/assessments will measure the network's vulnerability to:

- Inadvertent error or improper disclosure of information
- Fraud or theft
- Financial loss
- Harm to individuals from infringement of privacy rights
- Loss of proprietary information and harm to organisational activity

IT Services Response to Security Related Events

9.13.1 IT Services will make sure that security related events of which they are aware are promptly acted upon and related information will be documented.

9.13.2 IT Services will document corrective actions performed.

9.13.3 IT Services will record and report all computer system malfunctions together with problem resolution details.

Human Awareness of Security Issues

9.14.1 All Users must agree their responsibilities with regard to security, use of computer system facilities and use of information on the computer system.

9.14.2 Managers must ensure that appropriate guidance is given to users and administrators.

9.14.3 Individuals responsible for network computer system security and administration will have the necessary experience and will receive formal training in order to be able to perform their duties.

9.14.4 Social Engineering – Breaches of Information Security often now involve criminals using psychological means to circumvent security measures as well as the use of technical skills. Large companies and individual Internet users may be deceived into allowing criminals access to their computer systems, bypassing technical security defences. Such criminals making approaches by phone or in person may seem plausible and persuade the User to comply with their fraudulent requests. The victim, keen to appear helpful or intimidated by claims of authority or other pressures, may supply the criminal with information needed to break into the system either there on the spot or at some later time.

If approaches are made electronically, the victim may receive a message persuading them to click on a link, open an e-mail attachment or otherwise divulge information that they probably know, strictly speaking, that they should not. Users need to be aware of the risks and be wary of any unexpected approaches or occurrences.

All Users must be aware of these typical situations and exercise caution:

- **A computer becoming infected with a virus or Trojan after its User has been tricked into clicking on a link in the hope of getting something for free.**
- **Impersonation of authorised personnel with the intention of gaining access to restricted areas or to solicit information from staff.**
- **Pretending to be helpdesk/systems personnel/senior staff for the purpose of soliciting account information. Often for Bank and Building Societies but also corporate accounts.**
- **Any fictitious tempting offer to solicit a response, thereby confirming a "live" account which can be sold on to criminals who send "spam" email.**

9.14.5 Users must exercise caution at all times and immediately report any such suspicious activity to the IT Service Desk.

9.14.6 Responsibilities detailed above are delegated by IT Services to the appropriate system managers for non corporate systems.

10. PHYSICAL SECURITY

Physical security of the computer system, including central servers and workstations, is a critical aspect of IT security.

10.1 To maintain protection against intrusions, it is important that access to critical computer system components (such as the servers) is restricted to a small number of authorised individuals. Other considerations will include protection of equipment against theft, fire, and electrical hazards.

10.2 The corporate computer systems will be located in locked server rooms/Data Centers to which access is restricted to authorised IT Services staff and maintenance staff.

10.3 The corporate computer server systems will have adequate backup power for critical components.

10.4 Risers housing network equipment will be kept locked at all times with access restricted to authorised IT Services staff.

10.5 Workstations in public access areas will be provided with appropriate physical security and maybe monitored by CCTV surveillance equipment where appropriate.

10.6 Visitors to restricted areas should be supervised by authorised IT Services staff.

11. RECOVERY PLANNING CONSIDERATIONS

11.1 IT Services will maintain a detailed inventory list of all computer system components for corporate systems and ensure it is kept up-to-date. The inventory will cover servers, gateways, routers, hubs, Uninterruptible Power Supplies, workstations, specialised equipment, and backup media. The inventory will include the following information:

- Model and serial numbers
- Location
- Usage details
- Maintenance/ recovery procedure

11.2 IT Services will ensure adherence to backup procedures for all corporate systems. Other systems are the responsibility of the respective system managers.

11.3 System managers will design out any single points of failure where possible. Points of failure include weak links in software, hardware and data.

11.4 System managers will produce, test and maintain recovery strategies for all computer systems for which they have responsibility.

12. SECURITY ADMINISTRATION

Assigning administrative responsibilities for the computer system is absolutely necessary in order to maintain computer system security.

The System Administrator

12.1 The responsibility for the administration of the computer system, including security administration, will be assigned to knowledgeable individuals and authorised by the IT Services Manager.

12.2 The administrator will be aware of his/her responsibilities regarding administration of the computer system as well as the security and integrity of the data and information stored and processed on the computer system.

12.3 System administrators will be provided with the proper training, including training on security issues where required.

12.4 System administration external to the Computer Room will take place on secure workstations using secure IDs assigned to individual administrators as per the system administration rules.

12.5 System administrators will be aware that operational shortcuts can lead to errors and reduce effectiveness of safeguards or even negate them.

12.6 The College will maintain a keen interest in the work of appropriate national security bodies (e.g. the JANET Computer System Incident Response Team, CSIRT) to facilitate communication of current threats and countermeasures.

13. SERVER SECURITY CONSIDERATIONS

Subject to individual software implementation plan – will be different for each propriety software. System managers must consider the security of each individual server, and types of server, as part of the security of the computer system as a whole.

13.1 All use of a server will be prohibited unless the user has entered a valid User ID and password. Web servers may be exceptions if they are required to be publicly visible, but this will still depend on their exact purpose and content.

13.2 Backup systems will enable complete recovery of the entire server operating system, as well as data files in a timely manner.

13.3 Appropriate elements of hardware resilience (disk mirroring, server mirroring, load sharing on multiple servers) will be implemented for critical servers.

13.4 A standard, secure build will be developed by IT Services for each hardware/Operating System combination, and all will be built and maintained identically.

13.5 All Operating System security patches will be applied in a timely manner.

13.6 User accessible servers shall have anti-virus protection operating continuously.

13.7 Regular scheduled backups of the installed application software base will be taken to guard against file system corruption, damage, total loss and other contingencies.

14. USER IDENTIFICATION AND AUTHENTICATION

User identification and authentication is the ability to identify the User to the computer system and to confirm the claimed identity of the Users. The User identifies him/herself to the computer system by entering a User/Logon ID, usually consisting of his/her name. The User's identity is authenticated when the User enters a valid password.

User Registration

14.1.1 The corporate computer system will have User registration software for the creation of User IDs and allocation of resources to them.

14.1.2 There will be up to date procedures for the administration and usage monitoring of network UserIDs.

14.1.3 Users will be registered when proof of identity in the form of supporting documentation is provided according to User type.

User IDs

14.2.1 Each User will have one and only one User ID and the ID will be unique within the computer system.

14.2.2 Disabled User IDs will have their access to computer systems suspended and deleted dependent on criteria according to User type and timescale.

14.2.3 User types fall in to one of three categories; staff, student or external. The external category has an important subcategory of 'associate staff'.

14.2.4 Staff accounts are disabled at the end of employment and then normally deleted 1 month after the account is disabled.

14.2.5 Student accounts are deleted when meeting criteria set out in the EBS system. When this criteria is met the account is automatically disabled/deleted.

14.2.6 External accounts are deleted 1 month after they expire

14.2.7 Generic accounts are subject to limited access. Please refer to policy on Generic Accounts which includes application and authorisation process. Generic accounts will normally be valid for 5 working days, with a maximum life of one term where appropriate authorisation has been obtained.

User Passwords

14.3.1 User passwords must be known only to the User and the computer system.

14.3.2 The User's supervisor or the computer system administrator does not need to know a User's password and will not ask for it.

14.3.3 The User has no need to and must not divulge their password to another party.

14.3.4 Passwords will not be echoed to the User's screen when they are keyed in.

14.3.5 When a User forgets his/her password, the user can self-generate a new password using approved software. A temporary password subject to proof of identity, can also be provided if necessary in some instances. The computer system requires the User to change the administrator assigned temporary password as soon as they first log in.

14.3.6 The User will be required to follow good security practices in the selection and use of passwords. See Section 16, 'Use of Computers'.

14.3.7 If suspicion arises that a password may be known to an unauthorised party, the password should always be changed immediately and without regard to whether a regular periodic password change is due.

14.3.8 For network passwords, (and for all other software, where possible) the policy for staff access will be as follows:

- Minimum Length = 8
- Unable to use past 3 passwords
- Passwords changed every 60 days
- Cannot change password within 1 day of password changed
- Password Complexity – Password must contain 3 of the following:- Uppercase Letter, Lowercase Letter, Base 10 Digits (0-9), Non-alphanumeric (e.g. ! $ # %)

Periodic Changes of Password

14.4.1 Where technically possible, the computer system will require periodic changes of the User's password. This is currently six months for students and 60 days for staff.

14.4.2 The User will be required by the computer system to choose a password different to the previous three used.

14.4.3 Where technically possible, the User will not be able to use expired passwords as the new password when the system forces a password change.

ID Cards and Access Control Cards

14.5.1 Lost or misplaced corporate identity cards present a security risk. The information they contain may, in circumstances where either password security is inadequate or some deception is used, allow an intruder in possession of the card to gain access to live accounts. Consequently it can also mean that in some cases, College information or other significant parts of computer systems are at risk. The loss of cards used for controlling access to buildings or secure rooms can potentially lead to a breach of physical security. To guard against such events it is important that

- The User of such a card reports its loss to the place of issue at the earliest opportunity.

- Administrators handling a report of a lost card must immediately disable the card and revoke any access privileges associated with it on the relevant systems. This is so that the card will no longer be recognised as valid if used in an attempt to gain access.

- The User should be requested to follow relevant procedures for a replacement card to be issued.

14.5.2 When a lost card is found

- The card should be handed in to the place indicated on it.

- The User should be informed that the card has been found. If the loss has not already been reported, the user should also be requested to attend the relevant place for a new card to be issued.

- The lost card should never be returned to the User but a new one always issued.

- The lost card must be disabled on the relevant systems for the reasons outlined above.

- To help protect the personal information held on such cards, the old card must be destroyed and not disposed of intact to ensure that the Data Protection requirements are met.

VIRUS PROTECTION

Effects of Virus Infection on a User

15.1.1 Recent high profile cyber-attacks have proven to be capable of bringing down some of the world's most high profile computer systems. The risk to business operations is wide ranging. A virus infection may be, at a minimum, an annoyance to Users of a personal computer. However, in some instances, a virus may end up costing the User a lot of time through destruction of information or by preventing the User from being able to access the data stored on a hard drive. Increasingly likely is the possibility of a personal computer being infected but showing no outward sign. The compromised personal computer may behave in a way that impacts on its local network or may have effects on external sites by hijacking normal communication mechanisms for the virus propagation or other unwelcome activities.

System-wide Effects of Virus Infection

15.1.2 If an outbreak of virus infection is not well contained there could be major disruption including:

- Denial of service due to network traffic congestion from infected computers. The congestion may reach the point where communication over the network is no longer viable, especially over slow links to remote sites.

- The possibility of re-infection. Without adequate protection in place, previously infected and cleaned computers may become re-infected from executing programs in the central file store which carry the virus.

- Implications for the System Administrator. The system administrator may unwittingly be a major source of infection due to possession of system level access to the computer system or even just extended access rights to its file store.

- Should the spread of infection extend far enough, effective loss of the entire file system may be the result. The computer system as a whole might be considered too badly compromised to be repaired.

Protection measures

15.3.1 Virus scanning and cleanup programs are installed on the system file servers and workstation clients.

15.3.2 User files are scanned, on writing, to servers system wide to detect viruses.

15.3.3 The workstation client ant-virus software is configured to scan on writing files to the local hard drive, any other local storage including secondary hard drives, CD/DVD drives and USB memory sticks will be scanned on both reading and writing where technically possible.[1]

[1] The anti-virus software will attempt to clean infected files, but any infected files it cannot clean will be automatically deleted. This is to prevent the spread of infection.
To help guard against loss of work, the User is advised to possess more than one copy of any file they bring to the College from elsewhere, and not to rely on a sole existing copy brought in on a single USB memory device.

15.3.4 The anti-virus software will be updated regularly in order that it may detect new viruses.

15.3.5 Virus outbreaks will be monitored to determine if changed action is required as a result of a particular or new virus.

User Awareness of Virus Issues

15.4.1 Users will be warned that virus scanners are not foolproof and are largely reactive to new viruses, leaving a window of opportunity for new viruses before they are detected and incorporated in a scanner.

15.4.2 Users will always be careful to verify the source of computer based information. If a file is discovered to be infected the onus is on the User to notify all sources and destinations of the file to prevent further spread (and maintain goodwill).

15.4.3 Users must be particularly careful when distributing files, especially by email, to avoid spreading viruses. Unnecessary use of email attachments will be discouraged.

Responsibility for non-corporate College networks

15.5.1 The administrators of non-corporate systems will be responsible for anti-virus protection and scanning.

15.5.2 In the event of non-corporate College networks becoming infected, IT Services reserves the right to isolate such networks by disconnection if it is judged necessary to protect the corporate systems or external sites.

16 USE OF COMPUTERS

User Accounts and Passwords

16.1.1 Individual Users will each be given a personal account for which they are held responsible. The account is for the sole use of the authorised User for access to the College's IT facilities.

16.1.2 The account must not be used by anyone else and the password to the account must not be shared with any other person for any reason.

16.1.3 The User will be required to use passwords which are a least eight characters long and comply with password policy as set out in section 13.

Storage of Corporate Information

Any exceptions to the following rules on the storage of corporate information must be by agreement with the IT Services Manager, or nominee.

16.2.1 All College information must be stored on the network storage provided.

16.2.2 Non-encrypting USB memory sticks and external hard drives **must not** be used to hold College information including personal data, corporate confidential or otherwise sensitive information.
Any USB storage device used for College information **must** be an *encrypting* type approved by IT Services. College information must not be stored on such devices for longer than needed to complete transportation and transfer between systems.

16.2.3 Corporate documents and files should be stored in the appropriate shared folders, and not in e-mail systems or in users' private file store.

16.2.4 College information must not be stored off-site except by prior agreement with the IT Services Manager, or nominee.

16.2.4 Personal 'Cloud' based services must not be used for the storage of College information. Such services are run by third parties and are therefore outside the control of the College. Their security, Data Protection regimes, and terms and conditions may not match the College's own requirements. As in some cases the stored data might be accessible to employees of these services, to store College information on these services could amount to unauthorised disclosure of that information to the third party and be in breach of Data Protection legislation.

16.2.5 Where necessary to store College information elsewhere, a current copy must be maintained on College systems.

Mobile Computing (Laptops, Tablet Computers, Smartphones, PDAs etc)

The User is reminded that portable computing devices are frequently lost or stolen. Loss or theft of a device could result in a costly breach of information security if adequate protection has not been applied. This policy describes protection measures aimed at mitigating the effects of such a loss. However, the User is further reminded that they have primary responsibility to take care of the device and minimise the risk of loss or theft.

16.3.1 Encryption – points to note

- Any College information of any kind held on a portable computing device **must** be encrypted. ***It is the User's responsibility to comply with this requirement.***
- The User **must not** store College information on the device without encrypting it.
- Non-encrypting devices **must not** be used for the storage of College information of any kind.

16.3.2 Portable computing devices (such as laptops, tablet computers, PDAs and smartphones etc) must not be used for the *permanent* storage of information related to students, staff, external customers, and confidential or sensitive issues of any kind. Any copy of such information held on the device must only be *temporary* and **must be** erased after use. The User must ensure that all such information is securely encrypted whilst on the device, and also ensure that any portable device is disposed of in accordance with IT Services rules. Emails should not be used for sensitive information but they are particularly vulnerable on portable devices as they are often difficult to encrypt. Ensure sensitive emails are not used or retained at all on these devices.

16.3.3 For mobile devices such as PDAs or smartphones, the User **must** ensure the device PIN or password has been set, and that the device is set to automatically lock after a period of inactivity. This will help protect the device against misuse and is an extra safeguard for any personal contact details or any other confidential information held on the device should it fall into the wrong hands, but it does not replace the need for encryption. The User is reminded that any device without a PIN or password **must not** be used to hold any College information or confidential details.

16.3.4 The User is responsible for physically safeguarding the equipment against Unauthorised access, misuse, theft, or loss.

16.3.5 The User of the equipment must comply with the security requirements of this document at all times.

16.3.6 The User must comply with the Data Protection requirements at all times. See the above guidance on the storage of data, and the section "Data Confidentiality Considerations".

16.3.7 If College information is to be transported on USB memory devices, the User must

- Ensure any USB device used is an **encrypted/protected** type approved by IT Services.
- Take great care to ensure current files are not overwritten with old versions, and that incorrect or out of date information is not imported for processing.

Working from Home

This section is most relevant to staff members who undertake work from home and use their own home PCs to access the College's IT systems (eg Using VDi systems) . However, other Users should also implement the protection measures described in this section to best protect their own home computing devices.

When working away from the campus, Users needing to work with College information should use remote access (eg VDi) to access it where practically possible. This is much preferred over transporting College information on USB memory, which involves risk of theft or loss.

Other points to note -

16.4.1 Users are reminded that when using home PCs or other equipment at fixed locations outside the College, they are operating outside the College's IT security perimeter.
In these situations, users must not assume their own PC equipment is protected by the same security measures as standard PC equipment routinely used at the College and directly managed by IT Services.
Users must be aware that weak security on home PCs used for home working could lead to College account passwords becoming known to criminals, which could lead to security incidents involving College IT systems. It is vital that PCs used for home working are themselves properly secured, and it is the responsibility of the User to ensure that is so (see paragraph 16.4.4)

16.4.2 The User is responsible for safeguarding the equipment against unauthorised access, misuse, theft, or loss.

16.4.3 The User is responsible for ensuring that where the equipment is used by others (e.g. family members) that no College information is left open to breaches of corporate or personal privacy and that the equipment is not left in circumstances where other breaches of security may occur.

16.4.4 The User must ensure that all reasonable protection measures are in place and operating where applicable i.e.

- Firewall
- Anti-virus software that is set to automatically update itself
- Anti-spyware software to provide continuous protection against malicious software being downloaded
- Up to date security patches must be installed for both the operating system and applications when they are released by software vendors. Doing so will help protect the equipment against security vulnerabilities that have been identified.
- Wireless networks at home must be properly secured against eavesdropping and intrusion.

16.4.5 The User of the equipment must comply with the security requirements of this document at all times.

16.4.6 The User must comply with the Data Protection requirements at all times. See the above guidance on the storage of data, and the section "Data Confidentiality Considerations".

16.4.7 The network storage provided must be used for storage of College information, and must only be accessed by one of the currently approved methods. The home computer equipment itself must not be used as storage for any College information

unless in exceptional circumstances and by agreement with the IT Services Manager, or nominee.

16.4.8 When authorisation is given to store information on home/mobile devices, the User must encrypt the information in the manner prescribed by IT Services.

16.4.9 Protection measures for the equipment and the method of remote access may vary depending on the information being processed. Remote workers must follow the agreed security procedures at all times.

Use of Electronic Mail

Any exceptions to the following rules on the use of e-mail for transfers of information must be by agreement with the IT Services Manager, or nominee.

16.5.1 If there is no better option than electronic mail for the transmission of personal, confidential or sensitive information, the User **must** carefully ensure the message is correctly addressed. The possibility of misaddressing could mean the information is delivered into the wrong hands, and it is the responsibility of the User to guard against any such unwanted disclosures and comply with the Data Protection Act 1998.

16.5.2 If using electronic mail for the transmission of personal, confidential, or sensitive information, the User must follow the current guidance on whether to use encryption. The method of encryption is prescribed by IT Services.

Type of Scenario	**Is Encryption Required?**
Personal information about **1** person sent to **internal** email address	No, but the User **must** take care to use the correct email address
Personal information about **1** person sent to **external** email address (any address *outside* the College)	The user **must** follow the guidance in paragraph 4.1.5 on assessing the sensitivity of the information. If the risk is negligible then there is no requirement for encryption, but the User **must** keep information to the minimum required and **must** take care to use the correct email address. If the information to be transmitted is highly sensitive then the User **must** arrange with the recipient for the recommended encryption to be used.
Personal information about **many** people sent to **internal** email address	Encryption is advised. In any case, the User **must** take care to use the correct email address.
Personal information about **many** people sent to **external** email address (any address *outside* the College)	The User **must** arrange with the recipient for the recommended encryption to be used.

As evidence of good practice, Users are advised to retain email messages from information recipients discussing whether the recommended encryption can be used.
Queries concerning the above table should be addressed to IT Services on extension 2222 or by email at itservicedesk@colchester.ac.uk.

16.5.3 Many people now make use of mobile devices for email with greater risk of information disclosure through device loss. Contact the recipient when proposing to send a sensitive email to ensure they can receive it in a safe environment.

16.5.4 As stated in Section 4, “Data Confidentiality Considerations” paragraph 4.5.1, Users are reminded that electronic mail systems hosted by external providers are outside the control of the College. Such systems must not be used in pursuance of official College business or for the storage of corporate, personal, confidential or otherwise sensitive information.

Software

16.6.1 Copyrighted and licensed software may not be copied or distributed by Users in contravention of the licensing agreement.

16.6.2 It is not permitted to operate corporate workstations in an experimental manner. For example, by the trialing of software installed to a removable disk and/or modifying elements of the Operating System manually or by application download (screen savers, themes etc.)

16.6.3 Personal use of peer-to-peer networking and file sharing applications is not permitted on any of the College’s systems.

Concerns over this type of software include:

- Peer-to-peer software requiring an agreement from the end user to provide services to the peer-to-peer network using the College’s resources. Individual Users are not empowered to give such consent.
- Increased risk of virus infection over peer-to-peer networks.
- Spyware and other privacy risks as far reaching as full access to the computer’s hard drive.
- Legal risk due to storage of copyrighted material. Peer-to-peer software may store such material without the knowledge of the workstation User.

17 SYSTEM PLANNING

17.1 Proposals for new information systems, or enhancements to existing information systems, must be authorised by the IT Services Manager, or nominee. This is subject to security risk assessments, which must be made by suitably qualified IT Services staff.

17.2 Departments and Services must not contract digital services from external providers without the prior express permission of the IT Services Manager, or nominee.

17.3 Project leaders and managers must ensure security is considered at all stages of projects relating to information systems.