IT AND INFORMATION SECURITY POLICY

INTRODUCTION

The purpose of this Policy is to describe the procedures and processes in place to ensure the secure and safe use of the College's network and its resources and to protect College systems and data from unauthorised access or disclosure.

1. Scope

1.1 This policy is intended to be read by all staff for general information and awareness, and makes reference to more detailed information and guidance in additional specific policies.

1.2 The policy is relevant to all Information and Communications Technology (IT) services irrespective of the equipment or facility in use, and applies to:

1.2.1 All employees and visitors (with a temporary log-in) using the College's equipment and facilities.

1.2.2 All use of IT throughout the College.

1.3 In addition, all users of IT and other College facilities are reminded that there are elements of the Staff Code of Conduct which also apply.

1.4 The policy also takes into account the creation, management, processing and sharing of information. Therefore, this is an information security policy which incorporates use of IT (hardware and software), electronic communication (Email, telephone and fax) and issues relating to the storage and use of data, including confidential information.

1.5 The use of e-mail and the Internet are the subject of a separate policy.

2. Introduction

2.1 The College has a large investment in the use of IT which is used to the benefit of all staff and learners.

2.2 Throughout the College the use of IT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of all IT systems, and data, are maintained at a level which is appropriate for the College's needs.

2.3 <u>The policy has three main objectives</u>:

2.3.1 To ensure that all of the College's assets, staff, equipment and data are adequately protected against any action that could adversely affect the IT services required to conduct the College's business, and the accuracy and confidentiality of information held.

2.3.2 To ensure that all staff are aware of and fully comply with all relevant legislation.

2.3.3 To create and maintain within all departments a level of awareness of the need for IT and information security, to be an integral part of day to day operations and the responsibility of all staff to comply with this and other relevant policies.

2.4 This policy has been approved by the Corporation Board and must be read in conjunction with the College's Code of Conduct.

2.5 Additional related Policies include:

2.5.1 Email and Internet Policy, describing the acceptable use of the College's email system, its operation and its management.

2.5.2 Transportation, Transfer and Sharing of Data Policy, describing rules associated with personal and confidential data in transit, and procedures for transferring and sharing data.

2.5.3 Mobile Computing Policy, for those using mobile devices such as laptop computers.

3. Responsibilities

3.1 All staff, as users of the College's IT systems, are required to formally acknowledge receipt of this policy.

3.2 IT and information security is the responsibility of the College as a whole and consequently a responsibility of all members of staff and other authorised users. The policy has been approved and adopted by the Executive team. All staff and all users will take responsibility for their actions and ensure they do not put the college at risk.

3.3 All providers and users of IT services must ensure the security, integrity, confidentiality and availability of all data they create, process or use.

3.4 The College complies with all UK legislation which impacts on IT.

By conforming fully to this policy, users can be assured that they will be complying with the relevant legislation. See Paragraph 15 below for information on key legislation.

4. Breaches of this Policy

4.1 Any breach of this policy is viewed very seriously by the College and could lead to disciplinary action and/or prosecution as appropriate.

4.2 Violations of this policy will include, but are not limited to, any act, behaviour or actions that:

4.2.1 Involves the malicious use of data

4.2.2 Involves the disclosure of confidential information

4.2.3 Involves the sending of defamatory information

4.2.4 Involves the installation of unauthorised software

4.3 Any individual who has knowledge of a violation of this *IT & Information Security Policy* must report that violation immediately to the Director: IT. See the Reporting Security Incidents Procedure for more information.

5. Network Access

5.1 Access to the network, and any equipment, application, database or other resource must be by individual login – i.e. unique user name and password. Other than in certain circumstances, generic login credentials are not permissible except in particular circumstances where local need requires this e.g. in the Learning Resource Centres and Flexible Learning Centres.

5.2. All external use of the network must be by named individuals only, utilising the college remote access system (2X).

5.3 The creation of new staff accounts is carried out by the MIS team on receipt of data from the HR team. This is an automatic process.

5.4 Each individual who is authorised to access the College network is given a profile which limits his or her access to approved data, files and software.

5.5 If, for the purpose of a special project, an individual requires access beyond their normal profile permissions, special access can be arranged, but only for the duration of the project. Any request for a temporary or permanent variation from the profile must be made to the IT helpdesk and authorised by an appropriate line manager.

5.6. All users must only access, or attempt to access, what is permitted by their profile. If there is any difficulty in accessing files or programmes, the IT helpdesk must be informed as soon as possible.

5.7 If access to a file held in an individual's Home drive is necessary in the absence of an individual, then the line manager must contact the individual concerned to allow access to their Home drive and then contact the IT helpdesk for assistance. The reason for the access, the full name of the file, and the identity of the person holding it will be needed. In exceptional circumstances, access may be granted without the authorisation of the individual, e.g. they are off work sick and unobtainable.

5.8 As a principle, all users must retain their files on their Home drive. Should additional storage space be required this can be arranged via the IT helpdesk Please note that this space should not be used to store personal files e.g. music or photographs

5.9 Data stored on a local computer's hard drive is not automatically backed up, and may be accessible to anyone switching on the PC. A computer hard drive is therefore not secure and must be seen as a last resort and a temporary, short term solution.

5.10 Where a computer is shared by a number of users, it is essential for all users to log off the computer before leaving it. A user is responsible for all work carried out on a computer using their login details, including internet access and email use, whether or not that user was actually using the computer themselves. Users will not be held responsible where illegal access was found to be as a result of malicious software.

5.11 The network will require a password change for all staff every 90 days, but staff with domain admin accounts every 30 days.

5.12 Access may be suspended as part of any disciplinary action involving breech of this policy and those listed in Paragraph 2.5 of this policy.

5.13 <u>Segregation of Duties</u>

5.13.1 Access to systems and applications is restricted according to the role and business requirements of each user. Access rights are agreed by a user's line manager and the owner of the system or application.

5.13.2 Access to systems and applications is at all times by unique user ID. Group IDs are generally not allowed, except by specific agreement of the Head of: IT and Learning Resources, and where relevant, internal audit.

5.13.3 Within a system or application, segregation of duties must be implemented to prevent accidental or deliberate misuse. Duties or responsibilities which may give rise to a conflict of interest if carried out by the same individual must be separated.

5.13.4. Access rights are established through the New User/Change User process.

5.13.5. Established access rights must be reviewed twice yearly as a minimum to ensure that access to systems and applications remains appropriate and consistent. A review should also take place after any change to the system, such as an upgrade. This will be carried out by the Head of IT.

5.13.6. On receipt of a "Delete User" instruction, access rights to all systems and applications associated with that user must be revoked immediately. Weekly leaver reports from HR should also be checked against access permissions as a second check.

5.13.7. System Administrator access allows full unrestricted rights to defined systems and applications for management purposes, including the creation and removal of system users. This level of access must be kept to the minimum number of individuals required to enable day-to-day operation and emergency access in the event of a system failure. System Administrator access should be via unique individual ID.

5.13.8. The use of privileges in systems and applications must be allocated in a restricted and controlled manner. Privileges enable users to override some controls within a system, usually for system management purposes, and privileges must be removed when no longer required.

5.13.9 Access to systems and applications by third parties, such as partner organisations or software maintenance/support personnel, must be restricted to organisations where a written contract has been established for the delivery of those services and where appropriate a confidentiality agreement. Access by third parties must be restricted to only those systems, or parts of those systems, that are required and must be revoked as soon as it is no longer required. Access must be subject to approval and a confidentiality agreement.

6. Passwords

6.1 Passwords must be used in order to access computers, applications, systems and all other networked resources

6.2 Good practice would indicate that passwords should contain a combination of letters and numbers, and be at least seven characters of which at least one must be a digit. An alternative strong password can consist of four words, each more than 4 characters long. E.g. "barndoorblackhorse". Because it is longer this password is far more secure than "21W$qtz5" but much easier to remember.

6.4 The same password must not be used for more than one application, system, device or service

6.5 Staff with higher level access to college IT systems (Administrators) should maintain a personal account for everyday use and an administrator account that is only used when required for admin use. Different password must be applied to both accounts.

6.5 The network will prompt for a password change every 90 days.

6.6 In summary:

Strong Password Dos and Don'ts

DO	DON'T
Use a password with mixed-case letters	Use a your network login ID in any form
Use a password that contains at least one letter and number	Use your first, middle or last name or anyone else's in any form. Don't use your initials, nickname, or anyone else's
Use at least seven characters	Use a word contained in an English or foreign dictionary
Use a seemingly random selection of letters and numbers	Use information easily obtainable about you – phone numbers, car registration plate, pet names etc
Use a password consisting of four easy to remember words, each at least 4 characters long	Use a password of all numbers, dates or a combination
	Use a password that is largely the same as any previous passwords e.g. changing numbers on the end

6.7 If a software package comes installed with a default password, that password must be changed immediately after installation.

6.8 Passwords must not be posted in a location accessible by others (such as a note stuck to the monitor, under the keyboard or even in a desk drawer).

6.9 Passwords must NEVER be divulged to or shared with anyone else. There are NO exceptions to this, and if a password is disclosed, and therefore compromised the IT helpdesk must be contacted. If a user is asked for their password over the telephone by someone purporting to be from information services or any outside authority, company or organisation, it must not be given. The name and telephone number of the person requesting the password must be taken and the IT helpdesk must be informed immediately.

6.10 A machine must not be left unattended while logged onto a system and should be locked.

6.11 Where files or data need to be shared between individuals the data must be held in a networked, restricted shared team folder or other secure environment.

6.12 A log file of invalid login attempts will be maintained.

7. Physical Security

7.1 All hardware devices must bear an asset tag sticker, which must not be removed throughout the life of the device.

7.2 All desktop devices, e.g. PC, printer and scanner, must have adequate precautions taken to protect them against theft and accidental damage in addition to environmental threats and hazards. All manufacturer and supplier instructions and advice must be followed.

7.3 Security precautions should, in the first instance, concentrate on adequate building security and siting of the device in the office, and then may extend to simple lock down devices attached to a desk.

7.4 All IT hardware and software purchasing must be coordinated through the IT team. This ensures that equipment in use across the College is consistent, meets appropriate standards and is compatible with existing equipment and network resources.

Therefore, all purchases of hardware and software must be made through the Head of: IT and Learning Resources. Advice on hardware and software requirements is also available from the IT team via the IT helpdesk

7.5 All desktop computer equipment should be **turned off** (not at the wall socket) when not being used for an extended period of time.

8. Installation of Software

8.1 Software purchases must be coordinated through the IT helpdesk

8.2 Only software for which the College is licensed may be installed upon any College computer. Only staff with the appropriate rights will be allowed to install software on College PCs. A full inventory of all software and licensing will be maintained in the College's software asset management system.

8.3 If there is any doubt about software license or authenticity the IT helpdesk must be contacted before proceeding with installation.

8.4 Appropriate action will be taken against any user found to have installed software that is not properly licensed or if the software is being used contrary to its license agreement.

8.5 Modification to existing software is generally discouraged, and in any case must be progressed through the IT helpdesk

8.6 In certain circumstances College IT staff will evaluate new software on their PC to determine if it would be of benefit to the College. All managers must follow any conditions laid down by the software provider especially when the evaluation is completed. The the IT helpdesk must be contacted if there are any problems in following the set conditions.

8.7 Staff negotiating contracts, under which software is to be written for the College, must seek to ensure that suitable arrangements are made for copyright to be vested in the College wherever possible.

9. Security Incidents

9.1 <u>Security Incidents</u>

9.1.1 A security incident is a situation where the security of a PC, a system, an application or the network has been compromised, and may be from an internal or external source.

9.1.2 Examples would include users who have accessed data or material which their user profile should have prevented them from seeing, or perhaps accessed a system or application at a user level to which they are not entitled. It could also be the introduction of a virus to a PC and/or the network, or network access by an unauthorised user.

9.1.3 Any individual who becomes aware of a security incident must report it as soon as possible, to his or her supervisor and to the IT helpdesk.

9.2 Security Weaknesses

9.2.1 A weakness is a situation whereby potential for a security incident is identified. A PC may be left unattended, logged into a system without a password-protected screensaver or other locking procedure potentially allowing access by unauthorised users.

Further examples could be the inclusion of too many individuals in a system's Administrator profile or a lack of procedures for signing out laptops or other portable devices to individuals, potentially allowing unidentified and/or unauthorised use of the equipment.

9.2.2 A weakness does not have to be specifically IT-related. It could be windows left open close to portable equipment, or a PC monitor displaying potentially sensitive data positioned to face a window.

9.2.3 Any individual who becomes aware of a security weakness must report it as soon as possible, to his or her supervisor, and to the IT helpdesk.

9.3 Security Breaches and Violations

9.3.1 A security *breach* is an activity which causes or has the potential to cause the loss, damage or corruption of data. This may be the result of a specific security Incident, a security weakness, a violation of security policies or procedures or a combination of all three.

9.3.2 A security *violation* is any activity which contravenes the IT & Information Security Policy and other related policies, procedures and guidelines and may result in a security breach.

9.3.3 Any individual who has knowledge of a violation of this or other associated policies must report that violation as soon as possible to the IT helpdesk.

9.4 Any security breach or violation of this and other related policies could lead to appropriate action being taken against those who commit such a breach or violation. Violations and breaches will be addressed under appropriate procedures which may include the Disciplinary Procedure.

10 Virus Prevention and Control

10.1 A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus can also transmit itself across a network, spreading the infection to other computers and devices.

10.2 The general term is "malware", which covers various types of virus, worms, trojans, and spyware. A virus can cause performance problems or more long term damage to a computer or network.

10.3 Malware is most commonly introduced to a computer through internet downloads and as attachments to emails.

10.4 If a virus is found, or suspected to be on a machine or external storage media, the IT helpdesk must be informed immediately.

10.5 From time to time the IT helpdesk may notify users, through email, concerning a particular virus and its effect. All users must take appropriate action when so notified. Deliberate contravention of such a notification is a potential disciplinary matter.

10.6 Virus Prevention

10.6.1 No computing devices, whether desktop or portable, must be implemented on the network without appropriate anti-virus software being installed.

10.6.2 All software must be checked for viruses before installation on any College device, including computers, laptops and other portable devices.

10.6.3 If there is any doubt as to the origin of the files being transferred, they must always be checked for viruses before use.

10.6.4 Networked desktop PCs are updated automatically but other equipment such as laptop computers and other mobile devices need to be updated individually. the IT helpdesk can provide further information.

10.7 Downloading from the Internet

10.7.1 The downloading and installation of software from the internet is only allowed to designated staff with the appropriate rights.

10.7.2 More information on the use of the internet is available in the Email and Internet Policy.

10.8 Extracting Email attachments

10.8.1 Anti-virus software is installed on the College network and networked machines. This will scan all attachments for viruses etc

10.8.2 If there are any doubts about the authenticity or content of an email or its attachment the IT helpdesk should be contacted immediately for advice prior to opening the file.

10.8.3 More information on the use of the email system is available in the Email and Internet Policy.

11. Sending Confidential Information

11.1 More detailed information regarding confidential and personal information can be found in the Data Protection Policy and the Transportation, Transfer and Sharing of Data Policy

11.2 It is the responsibility of all employees of the College to safeguard the security of confidential and/or personal data for which they are responsible, or which they access in order to carry out their job. There is also a responsibility to bring to a manager's attention any areas of concern regarding the transfer or transportation of such information.

11.3 As a general rule personal and sensitive corporate data must not be disclosed, transferred, or copied to third parties without authorisation from an appropriate senior manager, who understands the purpose of the request and is aware of the procedures to follow.

11.4 Before making information available to anyone else, employees must make sure that they have the authority to disclose it.

11.5 Providing information by telephone

11.5.1 Information must never be given out over the phone or by any other verbal means unless it is absolutely clear who it is being given to and that they are entitled to the information and are ready and able to accept it.

11.5.2 Care must be taken to ensure that conversations involving confidential and/or personal information cannot be overheard.

11.5.3 Voicemail messages containing personal information should only be left after due consideration has been given to the security and confidentiality risks involved.

11.5.4 Recorded phone messages containing confidential information must be secured by password access.

11.6 Providing Information by Fax

11.6.1 If sending personal information by fax, pre-programmed speed-dialing must not be used, and top sheets must be clearly marked "Private and Confidential", together with the number of pages being sent and the contact details of the sender.

11.6.2 A confirmation sheet should be printed and filed as appropriate. The fax machine should also be checked to ensure that its memory does not retain a record of the transmission.

11.7 Providing Information by Email

11.7.1 Email is not a secure means of communication outside the security of the College's network and must not be used for sending personal or sensitive corporate data.

11.7.2 Even when emailing within the security of the College network it is important to ensure the name and email address of the recipient is correct and that a suitable subject line is used which does not include personal information.

11.7.3 The sender must also ensure that the recipient is expecting the information and confirm that it has been received successfully.

11.8 Providing Information by Surface Mail
Information transported by surface mail must be protected from unauthorised access and environmental damage. External organisations should be requested to use secure post when forwarding confidential information, using tamper-evident packaging when possible.

11.9 When using internal mail, confidential information must be placed in clearly identifiable envelopes and must be protected from loss and accidental viewing, using lockable storage equipment where appropriate.

11.10 Electronic data physically transported between sites, departments or organisations must be properly packaged and clearly labelled to ensure it is handled correctly, and not corrupted by magnetic fields or other environmental damage.

12. Termination of Employment

12.1 When a user who has network access leaves the employment of the College the appropriate manager must arrange for the transfer of any necessary files and e-mail folders.

12.2 The HR team will inform the IT team that the user is leaving so that the user's login credentials can be removed from the network. This removal will not take place earlier than 28 days after

the user has left to allow for the deletion or transfer of files, data and emails within the department. However the user's access rights will be disabled immediately.

12.3 On termination it is the user's responsibility to return all equipment, entry passes, software, documentation (both paper and electronic) and any other College asset in their possession.

13. Disposal of Media and Equipment

13.1 All PCs and data storage devices which have become obsolete or are surplus to requirement must be wiped clean. CDs and DVDs must be shredded before disposal.

13.2 The disposal of equipment is subject to the College's Financial Regulations and prior approval from the Director of Finance.

13.3 All removable media must be rendered unusable before disposal. (It should be noted that reformatting does not delete all data from disks and such data can subsequently be recovered using freeware.)

13.4 All magnetic tapes must be disposed of by a company or agency which meets Waste Electrical and Electronic Equipment (WEEE) Regulation standards.

13.5 All paper records can be disposed of through InPrint. However, paper documents containing confidential and/or personal information must first be shredded.

14. Audit and Review

14.1 IT and information security is managed through the Head of: IT and Learning Resources and is subject to regular audit and review.

14.2 The review process incorporates compliance testing of individual practices and procedures.

15. Key Legislation

15.1 Data Protection Act 1998

15.1.1 Further information about Data Protection is available in the College's Data Protection Policy, and also the Transportation, Transfer and Sharing of Data Policy

15.1.2 Data Protection refers to the principles and provisions of the Data Protection Act 1998, which seeks to govern the secure management of personal data, and in particular:

- The obtaining of personal data
- The storage and security of personal data
- The use of personal data
- The disposal and/or destruction of personal data

15.2 In Data Protection terms, personal data is information which would enable the identification of any living individual.

15.3 The Data Protection Act is based upon 8 principles, aimed at ensuring that all personal data is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary

- Processed in line with the rights of the subject of the data
- Secure
- Not transferred to other countries without adequate protection

15.4 The Computer Misuse Act 1990

15.4.1 This Act defines specific offences relating to computer “hacking”. Even the intent to make knowingly unauthorised access to programmes or data in a computer is an offence if the computer is made to perform some action (which can be as minor as scrolling the display).

15.4.2 Employees who themselves have authorised access do not have the authority to confer or authorise access on others.

15.4.3 It is an offence to incite anyone to confer unauthorised access.

15.4.4 It is an offence to cause unauthorised modification to programmes and data, which includes deliberately introducing a virus.

15.5 The Copyright, Design and Patents Act 1988

15.5.1 This Act specifies offences relating to the illegal copying of computer software.

15.5.2 All organisations have a legal responsibility to ensure all computer software is licensed by the vendor who holds the copyright to the product. Organisations are responsible for maintaining adequate records to prove compliance.

15.5.3 It has to be the policy of any organisation to ensure no copyright material is copied without the owner's consent.

This Act is enforced by organisations such as FAST (Federation Against Software Theft) and BSA (British Software Alliance) who have wide ranging powers to ensure compliance.

16. Training

16.1 Training will be offered to staff covering all aspects of the IT and information security policy.