SHREWSBURY COLLEGES GROUP

POLICY & PROCEDURE

INFORMATION TECHNOLOGIES ACCEPTABLE USAGE

1. AIM(s)

It is the policy and the intent of Shrewsbury Colleges Group ("SCG" or "the College"), to improve workplace and studying efficiencies by increasing its use of technologies related to information storage, transfer and retrieval. As necessary, SCG makes available its information technologies to its users. By definition a user is anyone who has access to and uses information technologies, systems and network infrastructure which are supplied by SCG and used on/off premise.

SCG encourages employees, associates and students to use the information technologies and achieve the efficiencies enabled by them. However, because of the nature of the information technologies, controls are needed to assist and protect both the College and its users.

This policy document will help to establish and reinforce safe and responsible online behaviour for all users and will cover the rules/regulations and best practice for safe IT usage. However it is just one aspect of a wider framework of e-safety, Safeguarding and Prevent strategies. For further information on this please refer to the Safeguarding Policy & Strategy, Prevent Policy & Strategy, Digital Life and the e-safety policy. For guidance on the usage of social media please refer to the Social Media Policy.

2. OBJECTIVES/STRATEGIES

Equality and Diversity - This Policy has been subject to an Equality and Diversity Impact Assessment. All individuals will be treated equally and fairly in the application of this Policy. All reasonable requests to accommodate requirements in terms of protected characteristics will be accommodated, as long as is it is practical to do so.
Scope - This policy applies to all staff and students at the College. This policy also applies to all volunteer workers, Governors, contractors, consultants, auditors, inspectors, agency staff, other visitors and students who have access to Shrewsbury Colleges Group information technologies.

Definitions - For purposes of this policy, "Information Technologies" shall consist of computer equipment, communication equipment, systems, and software provided by or through SCG to its users. Information Technologies includes any software, hardware, communications equipment deemed as 'Information Technology' by the Technical Services Manager. This policy shall also apply to any devices personally owned by the user to the extent that the devices are used for College purposes and/or are connected to the College network and/or external services via the College network. This particularly applies to users own devices connected via the college's wireless or wired networks (Bring Your Own Device – BYOD).

Privacy issues - Privacy is not expected. Authorised officials of SCG may access, at any time, any:

- data or files contained on any College provided or authorised computer drive or network share
- outgoing or incoming electronic messages
- any Internet transactions or usage on any College provided or authorised Information Technologies equipment, systems, or software.

Shrewsbury Colleges Group may disclose any such information to the extent permitted by law. Other than information that may be treated as confidential under Data Protection legislation, nothing on any Information Technologies equipment, system, or software shall be treated as private or confidential. The existence of passwords on any of the Information Technologies is not intended to indicate that messages, data, or files will remain private and users should not rely on this data remaining private. A user's use of any college provided Information Technologies constitutes the users consent to authorised access, and waiver of the user's privacy interest (if any) in, all messages, data or files.

The college may have to disclose certain information under the Freedom of Information Act upon receipt of an information request. The Freedom of Information Act gives anyone the right to ask any public sector organisation for all the recorded information they have on any subject.

Personal use at own risk - SCG understands that immediate family members or other friends and associates occasionally may leave or send electronic communications such voice mail or e-mail messages for a user. SCG is willing to accommodate such personal use of the systems to a limited degree; however, SCG treats such messages like other business messages and affords no personal privacy protections to them. Users should not have any expectations of personal privacy in anything created, sent, received, or stored on or by means of any of the Information Technologies.

Deletion or erasure not reliable: Even after a message, data or file has been "deleted" or "erased", it may remain on the system or be retrievable from a backup system. Therefore, users should not rely on the erasure or deletion of messages, data, or files to assume that it is "private" in any respect.

Password Security - A user shall not share their password(s) to any of the Information Technologies with anyone. Any user who shares his or her password(s) with anyone else is solely responsible for any damage or liability that may result. Accidental disclosure to another of one's password should be reported immediately to a Technical Services representative, and the user shall immediately change the password. Authorised technical support personnel may have to logon as a user for technical support purposes / fault finding. In such instances wherever possible this will be done with the user present, if not possible the user will be notified. To facilitate this the technical support person may change the user's password, the user will not be asked for and should not disclose their

password(s). As soon as the technical support person has finished the user should change their password immediately.

SCG maintained and controlled - Users are not to relocate or physically move desktop computers or any peripheral device. The Technical Services Manager must approve all moves. Only Technical Services Staff are authorised to move computers and related peripheral devices. SHREWSBURY COLLEGES GROUP PROVIDED INFORMATION TECHNOLOGIES ARE COLLEGE PROPERTY AND ARE INTENDED FOR OFFICIAL COLLEGE PURPOSES ONLY.

Records Retention - All messages, data, and files sent, received, created and/or stored on or through any of the Information Technologies are SCG property. The College is not responsible for loss or deletion of "personal" messages, data, or files on any of the Information Technologies. Users are reminded to clean out their email inbox, deleted items and sent items folders periodically to delete aged material and to move College critical documents to an appropriate folder on the shared network drive so that they are backed up. Electronic messages, data, and files should be stored and only be deleted in strict compliance with the College's records retention policy.

Purpose of use - The Information Technologies are intended for use by SCG users in conducting College activities only and not for the user's personal use. Users may not use any of the Information Technologies to solicit or conduct non-College business ventures, for political activities, extremism, to propagate malicious communication or canvas support for views, beliefs or activities detrimental to the Colleges' operations, potentially offensive to the views and beliefs of others or for any activity that is prohibited by law, regulation, policy or contract. Incidental and occasional personal use of the Information Technologies is permitted. However, a user's personal use shall not interfere with any user's productivity or performance, and shall not adversely affect the efficient operation of the College or the Information Technologies.

Intellectual property - Any documents contained on or created using Shrewsbury Colleges Group information technologies are the College property. Users may not reproduce or otherwise use any information received through e-mail or other Internet access that may unlawfully infringe upon another's lawful intellectual property (copyright, trademark, or patent) or other rights.

Note that the transmission of material which violates any copyright restrictions is also explicitly prohibited by the JANET AUP and is illegal - many commonly available digital media files such as MP3, MP4, WMV, AVI, etc. have copyright restrictions. The storage of copyrighted digital media files is not allowed on any college storage medium or systems other than where specific permission from the copyright holder has been secured or the materials are covered by a 'fair usage' policy.

The scanning or copying of documents in violation of copyright laws is also prohibited.

User Responsibility - Once a user "signs on" via his or her password, the user is responsible for all communications sent or data/files created or edited under that user's password. Therefore, any user who is "signed on" should be careful to not leave the workstation unattended for an extended period of time. Users should "sign-off" or lock the computer any time the user is away from his or her workstation. Users should make sure that they logout of any online systems before returning tablets or portable device as users can remain logged on to such devices even when they have been switched off. It is the responsibility of the user to safeguard their logon credentials and make sure that they are not used by anyone else.

All users should take full responsibility for their conduct and observe and model the British values of individual liberty, rule of law, democracy, mutual respect and tolerance.

Staff are required to demonstrate high standards in their exercise of authority, their management of risk, in the proper use of resources and in the active protection of learners from discrimination, radicalisation and avoidable harm. The duty of staff is to have due regard for the need to prevent people from being drawn into terrorism.

Non-affiliated access prohibited - No user may grant or permit any non-employee or student (including volunteers, Governors, clients, contractors, consultants, auditors, inspectors, agency staff, visiting lecturers, other visitors and students) to access any Information Technologies, or the messages, data and files contained thereon, without prior written approval of the Technical Services Manager. This statement also applies when accessing the college's network via guest wireless networks, offsite working and from home.

Message access - Messages on any of the systems are to be accessed only by:

- the intended recipient or author
- others at the direct request of the intended recipient or author
- Shrewsbury Colleges Group designated representatives

Therefore, users may not access another person's messages without either the other person's permission or a College related reason for doing so.
Any attempt by an unauthorised person to access messages on any of the systems (such as e-mail) is a serious violation of College policy. Any user who receives a message for which the user is not the intended recipient should either: 1) return the message to the sender and tell the sender of the error, or 2) forward the message to the intended recipient, if possible, and tell the sender of the error.

Data and file access - Data and files contained on any of the Information Technologies are to be accessed only by those users who have an official need to know about the information. "Browsing" through SCG data or files (in hard copy or electronic format) without a legitimate College related reason is prohibited. Any attempt by an unauthorised person to access data or files on any of the systems is a serious violation of College policy

and may also breach the terms of the Computer Misuse Act (1990) and/or Data Protection legislation.

Harassment and discrimination is prohibited - All usage of the Information Technologies shall comply with all UK laws and all College policies which seek to prevent workplace harassment and discrimination. For example, electronic mail, screen savers or wallpaper display that may create or could be perceived to create an offensive or a sexually hostile environment will not be tolerated. Any offender may be subject to the appropriate College disciplinary policy. For Associates and non-college employees this will be actioned by the appropriate agency, association or organisation and the College may immediately withdraw access to College-supplied information technologies.

Computer maintenance and backups - Users are responsible for managing the files stored on their hard drives and keeping them free of unnecessary data and files. Users who are issued portable computers such as a notebook, laptop or netbook, and users who use handheld devices such as tablets and Smartphones, shall perform all appropriate backups and destroy all data, files, and backup tapes in accordance with this policy and College' Records Retention policy. Users are required to store files on College' file servers rather than the local hard drive of the individual's personal computer where those files are considered business critical or where unintentional loss of those files would involve the user and therefore the College in additional work to re-create them. If the user does not have access to a file server, it is the responsibility of the user to backup his/her critical data files. SCG is not responsible for the loss or destruction of data stored on such devices. This also extends to the use of Bring Your Own Device (BYOD).

Authorised Software - Shrewsbury Colleges Group will not permit the existence of non-College owned or unlicensed software on any of its computers. Users may not copy, reproduce, download shareware/screen savers, digital media files (MP3, MP4, MWV, AVI etc. unless specifically related to College operations) or install any College licensed or owned software. Users shall never use any college system to distribute computer software or copyrighted media from any source. Users shall not install any software or Apps on college computers/devices unless authorised to do so by the Technical Services Manager.

Personal software: Installation of a user's personal software on any College computer is prohibited.

Virus Prevention - Shrewsbury Colleges Group maintains and uses comprehensive virus prevention software. All users must help in not compromising our prevention efforts or creating the possibility of a virus being introduced into the College computer system. Viruses can be introduced into systems through various media including personal software (games, in particular), USB devices, e-mail, CD/DVD ROMs, and the Internet. A virus's potential hazard to College computers and network requires that all users must:

- use and never bypass, College provided anti-virus software
- never install or use personal software

- never connect to or download files from any unauthorised Internet sites

All virus incidents must be reported to Technical Support Team, but users are NOT to forward suspect emails. Users responsible for a computer system that is not capable of receiving software updates automatically, are personally responsible for keeping the anti-virus software and virus definition files updated to the latest version. When connecting an external device such as a USB drive to a computer all files on the external device (including sub folders) must be virus checked before being opened, copied, moved or accessed in any way. It is not permitted to run computer programmes or software direct from an external device.

If users are using their own device (BYOD) to access network resources then it is their responsibly to make sure that the device is properly secured i.e. latest Operating System updates/patches, has adequate firewall protection, anti-virus software with up to date virus definitions and anti-malware software etc. Failure to comply with this may lead to the device being prevented from accessing the College network.

Internet usage - Access to the Internet by means of any College computer shall be for SCG business purposes only. All Internet usage is subject to filtering, logging and monitoring by College authorised personnel, this includes the content of Internet searches. Any attempt to gain unauthorised access to the Internet or blocked websites is prohibited. This includes trying to bypass the College's Internet filtering system. Accessing (or trying to access) proxy sites is not allowed. Any violation may result in the removal of Internet access privileges.

The Joint Academic Network (JANET) is the collection of networking services and facilities that support the computer communication requirements of the UK education and research communities. The college must ensure that unacceptable use of JANET does not occur by complying with JANET's own Acceptable Usage Policy. Failure to comply with the JANET Acceptable Use Policy may result in services being withdrawn from the Institution. All users accessing the Internet via the JANET network should make themselves familiar with the JANET Acceptable Usage Policy.

Guest Wireless Network - The College has undertaken a great deal of testing to ensure the integrity of this system. However through joining this network you are sharing a common space in which devices unknown to the college may reside. Unknown devices may not be as well protected as college systems from viruses and other malware and therefore could pose a risk to your device.

In the interest of protecting your device we recommend that a software firewall is enabled at all times (Windows / OSX both have one inbuilt) and that you have a recognised antivirus application running and up to date. While problems are unlikely, it is important to note that the college cannot assist with any issue arising from the use of this system nor accepts any liability for said issues. In addition the college cannot offer any support for equipment not owned by the College. Please do not use the College's network or systems if you are

unsure how to protect your personal devices or where the above statement is unacceptable. Usage of the college's wireless networks may be monitored and action taken against those who misuse the facility.

If users are using their own device (BYOD) to access network resources then it is their responsibly to make sure that the device is properly secured i.e. latest OS updates/patches, has adequate firewall protection and anti-virus software with up to date virus definitions, anti-malware software etc. Failure to comply with this may lead to the device being preventing from accessing the college network.

Electronic Messaging including E-mail – Any electronic messages created or sent on College systems shall not violate College policies against unlawful harassment or discrimination. Users may not use college systems to solicit or conduct non-College business ventures, to propagate malicious or defamatory communication or canvas support for views, beliefs or activities detrimental to the College operations, potentially offensive to the views and beliefs of others or for any activity that is prohibited by law, regulation, policy or contract. Sending "chain letters" (such as those requesting the recipients to send out a specified number of copies) is prohibited. If you chose to use a third party or web based email system from the college's network infrastructure including messaging facilities within social networking sites such as Facebook & Twitter then you do so at your own risk and must be responsible for your own usage, the college will not be held responsible for misuse of such systems.

In addition, all E-mail is subject to filtering, logging and monitoring by the College. E-mail shall be used intelligently, professionally, and conservatively. E-mail documents are essentially no different than any other typed or written document. The conduct of a user who sends email containing a College domain address (i.e. @shrewsbury.ac.uk or @SSFC.ac.uk) may be perceived as reflecting on the character of Shrewsbury Colleges Group, and all its users. In sending e-mail documents, users shall exercise the same discretion and professionalism required of any business communication. Users shall regularly review their e-mail files. Users are encouraged to delete unnecessary email as soon as possible. Email should be archived or otherwise backed up by the user as the college does not offer central backup and restoration.

Offsite users and home workers - Users who perform College work at home or anywhere else outside of College premises must observe all of these policy provisions, except as otherwise noted. Any College work, regardless of where or how created, stored, edited, sent, or received, shall remain SCG property at all times.
Any such messages, data, and files that are SCG property are to be archived in accordance with the College Records Retention policy.

If using computers off site or at home to connect to college systems then all feasible steps should be taken to prevent others from gaining access. This includes best practice steps such as locking the screen or logging off when not being used, keeping usernames and passwords secure etc.

Data Security & Data Loss Prevention - We have taken all feasible steps to make sure that our data is secure, but one very weak link in the chain is data that is taken from our systems and copied / moved onto removable media such as portable USB devices, Smartphones, CDs / DVDs or stored on portable IT equipment such as Laptops, Netbooks & Tablets, this also applies to Bring Your Own Device (BYOD).

To secure such data the College has made it mandatory to only use encrypted devices when 'personal data' is concerned. Therefore if you copy / move any personal data onto removable media such as CDs / DVDs or devices such as USB memory you must make sure that the data is encrypted. All laptops, Netbooks, containing Personal data must have the entire hard disk drive encrypted. All new College laptops etc. will be issued to staff pre-encrypted. All portable devices such as Smartphones and Tablets that are used to store personal data (including access to college email and cloud storage) must be protected by power on security system measures such as access pin, pattern, biometric etc and must be encrypted.

Users should use two factor authentication to secure mobile devices such as Tablets and Smartphones if said devices are used to access personal/sensitive data including email.

Users should not copy or download Personal data to privately owned devices, this includes portable devices such as Smartphones and tablets and also desktop computers such as Windows PCs, Laptops and Apple Macs that are located off site such as at home.

According to Data Protection legislation if you answer YES to any of the below question then the data is classed as personal:

Can a living individual be identified from the data?

Does the data 'relate to' the identifiable living individual, whether in personal or family life, business or profession?

Is the data 'obviously about' a particular individual?

Is the data 'linked to' an individual so that it provides particular information about that individual?

Is the data used, or is it to be used, to inform or influence actions or decisions affecting an identifiable individual?

Does the data have any biographical significance in relation to the individual?

Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?

Return of property and cancellation of use - Upon termination of employment or end of contract, or at any other time when requested by Shrewsbury Colleges Group, all:

- College issued Information Technologies equipment must be immediately returned to the College
- prior authorisations to use any of the Information Technologies or systems shall immediately cease and be revoked

Disciplinary Action - Users who violate this policy or associated legislation / law may be subject to:

- College disciplinary policy as appropriate (up to and including termination of employment or expulsion from study)
- Personal responsibility for any civil liabilities or criminal penalties
- discipline in accordance with the procedures of the contracting organisation (for associates)
- reimbursing Shrewsbury Colleges Group for any reasonable costs

Administration – Shrewsbury Colleges Group retains the absolute right, in its sole discretion, to change this policy and to determine whether a users' actions are covered by this policy. Any revised policy will be published to those affected via standard communications channels.

If a user fails to comply with any section of this policy, SCG may take whatever action it determines to be necessary to avoid or prevent further violations or harm to users, third parties, or College property. Such action could include removing access to systems (i.e. Internet access), disciplinary action, up to and including termination of employment or expulsion from study, as well as civil lawsuits or criminal prosecution.

Questions about this policy should be directed to the Technical Services Manager.

ACKNOWLEDGEMENT STATEMENT

My signature below indicates that I have read, understand and agree to comply with the document entitled, “SCG Acceptable Usage Policy on Information Technologies”.

I acknowledge that this signed form will be stored by the college for future reference.

SIGNATURE: _____

NAME (Please Print): _____

FACULTY / DEPARTMENT, ASSOCIATION or COURSE:

_____

DATE: _____