Shrewsbury School's Policies Concerning the use of Computers - Non-Pupil

The Director of IT Services is responsible for the formulation and review of policies affecting the use of computers within the School. These policies include co-operation with outside bodies such as the ICO, the Health and Safety Executive and the British Computer Society to ensure that the policies reflect current best practice and comply with any laws or regulations controlling the use of computers. These policy documents are subject to review by the Senior Leadership Team but ultimate responsibility for their content rests with the Headmaster and the Bursar.

All users of the School's IT systems are required to comply with these policies when using computers owned by the School or other computers when used for work on behalf of the school or on school premises.

General Rules

The general rules are posted in every computer room and on the intranet and are subject to alteration as circumstances dictate. In general, everyone is expected to use the facilities provided in a reasonable & responsible manner and behave in such a way as to permit everyone to work to their best advantage.

Health & Safety

The hazards associated with computing are relatively minor and are assessed by the Director of IT Services acting under the guidance of the School's consultants. Much of the legislation concerning the use of equipment, ergonomic considerations, eye tests etc are not applicable to 'occasional' PC users.

Confidentiality

Every effort is made to protect the security and confidentiality of information stored on the networks. This has to be balanced against the School's responsibility to maintain internal rules and regulations and to comply with any relevant laws.

Copyright

The ownership of work produced by staff and pupils can sometimes be in doubt. The School's policy is to interpret the law as generously as possible in favour of the author while retaining the rights only to such items as are covered specifically by this policy.

Computer Misuse Act

The unauthorised use of computers is a criminal offence. The Computer Misuse Act of 1990 formalises this and explains the different offences and penalties.

Use of Personal Equipment on the School Network

Use of personal equipment on the school network is permitted via the separate non-pupil VLAN; personal devices should not be connected directly to the school network. Personal devices should have no unlicensed or illegally copied software (including music and other data files) on it and you should be aware that you are still using school network systems to connect to the internet.

Acceptable Usage Policy

This policy applies to all non-pupil users of the School's IT facilities and sets down the standards which users are required to observe in the use of the IT network, email and the internet.

Non-pupil users include teaching and support staff, children and partners of residential staff, visiting adults and children and any other user category not defined as a pupil of the school.

Access for non-school related purposes is provided on a best efforts basis and subject to normal security and firewall rules. Shrewsbury School cannot compromise network security to accommodate personal preferences or requirements.

Deliberate access of inappropriate material by employees or visitors through school systems would be regarded by the school as a significant breach of trust, or, for certain materials or sites, gross misconduct, which may result in the school taking disciplinary action.

It is the responsibility of all users to acquaint themselves and comply with this policy. Certain terms in this policy should be understood expansively to include related concepts:

School includes all Shrewsbury School locations and both academic and non-academic areas.

Document covers just about any kind of file that can be read on a computer screen as if it were a printed page, including the HTML files read in an internet browser, any file meant to be accessed by a word processing or desk-top publishing programme or its viewer or any other electronic publishing tools.

Graphics includes photographs, pictures, animations, movies or drawings.

Display includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

The acceptable usage policy is split into seven sections:

- Internet
- Contacting Pupils
- Email
- Security
- Copyright
- Use of Technology in Classrooms
- Audio and Visual

By logging on to the Shrewsbury School network you signify your acceptance of this policy, and you should seek clarification of any issues that you do not understand.

Internet

Use of the Internet by non-pupil users is permitted and encouraged where such use is suitable for school purposes and supports Shrewsbury School's aims. In addition, at specified times and locations, you may access the facilities for personal activities including communication and recreational use. Personal use should never compromise availability for academic use.

The Internet is to be used in a manner which is consistent with Shrewsbury School's standards of professional business conduct and as part of a pupil's academic research:

During School hours we expect you to restrict your Internet usage to School related purposes only or to use the facilities in such a way as not to impact on overall performance – for instance, not to download large files or use streaming media excessively.

All existing School policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with privacy, misuse of School resources, sexual harassment, fraud and information security and cyberbullying.

Any file, including e-mails, that is uploaded or downloaded must be scanned for viruses before it is run or accessed. This should be done automatically, so non-pupil users must check that their antivirus software is running. Ask for advice from the IT department if you are unsure how to do this.

The School's Internet facilities and computing resources must not be used knowingly to break the law. Use of any School resources for illegal activity is grounds for immediate action and the School will co-operate with any legitimate law enforcement agency.

Any legal and licensed software or files downloaded via the Internet into the School network become the property of Shrewsbury School. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

- No user may use School facilities knowingly to download or distribute pirated (illegal and unlicensed) software or data.
- No user may use the School's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the security of staff or pupils.
- No user may use the School's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door programme code.

Non-pupil users are specifically prohibited from downloading any software onto School owned devices without the express permission of the IT department.

Users with Internet access may not upload any software licensed to the School or data owned or licensed by the School without explicit authorization from the member of staff responsible for the software or data.

The School's monitoring system (SmoothGuardian) records (for each and every user) each web site visit, each chat-room, newsgroup or e-mail message and each file transfer into and out of its internal networks. No one should have any expectation of privacy as to his or her Internet usage. The IT department will review internet activity and analyse usage patterns, and may choose to publicise this information to ensure that School internet resources are devoted to maintaining the highest levels of productivity.

Users should not download or view material that is obviously libellous (or otherwise unlawful), or inappropriate in any way, i.e. graphic images, sound files, or music.

Shrewsbury School reserves the right to inspect any and all files stored on School computing facilities in order to assure compliance with this policy.

The School has in place a firewall to ensure the safety and security of the School's networks. Additional devices may also be installed in the future to further protect these networks. Any user who attempts to disable, defeat or circumvent any School security facility will be subject to disciplinary proceedings.

Any files containing sensitive or confidential School information that are transferred in any way across the Internet must be encrypted. Advice and assistance may be sought from the IT department.

A USER WILL BE HELD ACCOUNTABLE FOR ANY BREACHES OF SECURITY OR CONFIDENTIALITY

Shrewsbury School's policy prohibits the sharing of User IDs or passwords obtained for access to Internet sites unless of an academic nature and unless the sharing has been approved by the Director of IT Services.

Contacting Pupils

If you need to contact pupils electronically you should use the school email system - the school system manages an "audit trail", for your protection, which is not necessarily present in other systems.

Do not respond to invitations from pupils in social networking sites. It is expressly forbidden for members of staff to be 'friends' (or the equivalent terminology) with pupils on social network sites.

Be aware of the professional risks involved in communicating with pupils via instant messaging mobile phone, text messaging or other messaging type mediums – though the school recognises that there are situations (for example on school trips, emergencies, or where an immediate response is required) where there is no alternative.

Where possible, staff should use school owned devices to communicate with pupils.

Email

All users need to be aware that e-mail carries exactly the same status as other forms of communication, including letters, memos and telephone conversations, and the same consideration and legal implications need to be applied and observed in the use of e-mail as in these other forms of communication.

The definition of Email covers:

i. Electronic Mail services within Shrewsbury Close Local Area Network (internal e-mail).

ii. Electronic Mail sent through the Internet to other organisations/individuals (external e-mail). iii. The safeguarding of information sent by e-mail.

The School provides an e-mail system to support its academic activities and access to e-mail facilities for all users is granted on this basis. In addition non-pupil users may use these facilities for personal activities including communication and recreational use. However, users are reminded that e-mail sent and received on the School's systems are not private property they remain part of the School's information systems. Personal use should never compromise availability for academic use.

When composing and sending an e-mail, it is expected that the content meets the standards of professionalism which Shrewsbury School expects of everyone.

It is not permitted to send sexual, racially biased or other inappropriate e-mails, which would infringe the School's code of conduct. Do not use aggressive, abusive or deliberately anti-social language. Never e-mail hastily or out of anger.

Use of personal e-mail must not detrimentally affect the duties of other email users or disrupt the system, and/or harm the School's image or reputation.

You should not copy or download or forward material that is obviously libellous (or otherwise unlawful), unrelated to work, or inappropriate in any way, i.e. graphic images, sound files, or music.

Access to Internet or web-based e-mail (i.e. Hotmail or Yahoo mail) is permitted, however be aware that this mail is insecure and may present a security threat.

Users are reminded that they are responsible for their own e-mail housekeeping. Unwanted e-mail should be deleted. If you are unsure how to achieve this, guidelines are available from the IT department.

Those with school email addresses should not give their external e-mail address out carelessly. Only enter it on business circulars and application forms if you are sure that it will not be misused or forwarded on.

Particular attention should be paid to the addressee to ensure the message will reach the intended recipient especially if choosing from an address list of similar names. You should, generally make use of the Global address book for all internal email addresses.

Messages intended for another recipient should be re-directed and then deleted. Any incorrectly addressed messages should only be forwarded to the intended recipient if the identity of that recipient is known and certain.

Security

Users should not allow other people to use their network login. Do not leave your PC logged on to the network. As a standard the School uses a password protected screen saver.

Anti-virus software is installed on every PC connected to the School's network. Anti-virus software must not be disabled or uninstalled for any reason. The anti virus software is set up to regularly scan each PC for viruses. If you notice that your anti-virus software is not running or scanning, you should immediately report the fact to the IT Department.

It is extremely common for a virus to propagate itself via an e-mail attachment. Commonly the attachment will be an executable file (with .exe, .vbs suffix). If there is any doubt as to the authenticity of an e-mail attachment, it must not be opened; report it to the IT department immediately.

It is also common for a virus to use the Outlook address book to forward itself to others. This means that infected e-mail could be received from a known and trusted source. You should be immediately suspicious if the email is unusual in any way.

Shrewsbury School maintains the right and ability at any time and without prior notice, where justified, to inspect any information stored on School computing facilities in order to ensure compliance with the policy.

If clarification of any aspects of policy are required, refer to the Director of IT Services.

Copyright

Every piece of work created belongs to someone. This includes text, images and any other form of intellectual creation regardless of how and where it is stored.

The majority of the software used within the School is owned by or licensed to Shrewsbury School and is protected by various patents, copyright and licence laws currently in force.

The copyright ownership of all material must be respected and the wishes of the copyright owner are to be observed.

No material may be copied from the Internet or any other electronic source save with the specific permission of the copyright owner. Stringent laws apply, in particular, to the scanning of material. The use of all such material is to be properly attributed.

No-one is permitted to make copies of or changes to any software owned by or licensed to Shrewsbury School except where specific permission has been granted so to do. This includes any upgrades, 'plug-ins' or new versions regardless of the source.

The copyright of any material that is commissioned by Shrewsbury School, produced as coursework or for which remuneration or other consideration has been given by the School, is the property of Shrewsbury School.

Scanning or digital manipulation of documents, diagrams, photographs etc that are copyright may be done only with the express permission of the copyright holder and in accordance with current law.

Use of Technology in Classrooms

This part of the acceptable usage policy has been produced to be read in conjunction with the School's Acceptable Usage Policy, the Pupil Behaviour Policy, the Anti-Bullying Policy, the Cyberbullying Policy, the Yellow Card and the Child Protection & Safeguarding Policy and Procedures document.

As in all areas of School life, the use of technology for Teaching & Learning purposes should be responsible, respectful and legal.

All technology brought to the classroom (or used for learning in houses or elsewhere on or off the School site) should not cause distraction or disruption either by accident or by design. Devices should only be switched on and accessible when teachers give instructions to that effect.

The School considers inappropriate use of technology in the classroom to be all activity that does not form part of the task as instructed by the teacher. This may include, but is not restricted to the following: gaming, emailing, texting or messaging, taking recordings or photos, using social media, using unsuitable apps and webpages.

Pupils who use technology inappropriately should expect the privilege to be removed and the device to be confiscated for a period of time. Additional sanctions may be considered in light of any other possible contraventions of related School policies.

CONFISCATION OF TECHNOLOGY PROTOCOL

Teachers should aim to ensure that the use of technology in the classroom is managed to be on task and always responsible, respectful and legal. Teachers should feel able to use their discretion as to what constitutes a distraction or disruption to the effective delivery of a lesson and whether it was accidental or intentional. If it is felt that confiscation of technology is appropriate, then the following protocol should be followed:

1) The teacher asks the pupil to switch off the device before handing it in.
2) The teacher checks that the device is switched off.
3) At the earliest opportunity the teacher informs the housemaster / housemistress via email that the device has been confiscated.
4) The device is handed in person to the housemaster / housemistress or placed in a marked envelope and placed in the appropriate locker.
5) Depending on the length of confiscation period, the housemaster / housemistress will contact the pupil's parents to explain that alternative contact methods will be required until the device is returned.
6) Housemasters / Housemistresses should keep a record of the above and keep the phone in a secure location during the time that it is confiscated.

Audio and Visual

In order that staff may understand the guidelines given to pupils in respect of Audio Visual devices, the relevant part of the Pupil AUP is reproduced here:

> "Pupils must not capture still or moving images or audio recordings of pupils or staff without their express permission. This includes capture with their own or a school owned device or by downloading from the intranet or internet.
>
> Pupils must not manipulate or edit content for which they do have permission in such a way as to embarrass, harass or cause offence to the person(s) recorded in the images or audio.
>
> Pupils are not permitted to upload any images or recordings to social media, other web sites or to share with other individuals or organisations unless they have been given permission to do so by the person(s) represented in the images or audio."