
# Shrewsbury School

# Pupil Acceptable Usage Policy

The Director of IT is responsible for the formulation and review of policies affecting the use of digital devices within the School. These policies include co-operation with outside bodies such as the Data Protection Registrar, 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 and other digital devices. These policy documents are subject to review by the Senior Leadership Team and the Designated Safeguarding Lead is responsible for the safeguarding content of the policies.

All students are required to comply with these policies when using digital devices owned by the School or other digital devices when used for work on behalf of the school or on school premises. These policies also apply to such use off school premises if the use involves pupils or any member of the School community or where the culture or reputation of the School are put at risk.

For the avoidance of doubt the term computer applies equally to all electronic or digital devices in use by pupils.

## General Rules

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

Failure to comply with these AUP will potentially lead to sanctions in line with the Pupil Behaviour Policy. Bullying incidents involving the use of IT will be dealt with under the School's Anti-bullying Policy. Unacceptable use of digital devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with the School's Conducting a Search and Confiscation Policy.

In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's Child Protection and Safeguarding Policy and Procedures).

In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to the Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

## Health & Safety

The hazards associated with Information Technology use are assessed by the Director of IT acting under the guidance of the School's consultants. Appropriate risk assessments are carried out. The instructions and guidance provided to pupils must be followed and pupils should report any issues of concern to a member of staff. Staff must then refer the matter to the Director of IT or Designated Safeguarding Lead

# Pupil Acceptable Usage Policy

## Confidentiality

Every effort is made to protect the security and confidentiality of pupils' work 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 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.

## Data Security and Backup

Pupil data held on the network is regularly backed up. However data on pupil personal devices is the responsibility of the pupil and they should make adequate arrangements to regularly backup important information. Advice can be sought form the IT department on a suitable regime if required.

## Monitoring and review

All serious incidents involving the use of IT will be logged centrally by the Designated Safeguarding Lead and the Director of IT.

The Director of IT will monitor the use of IT as set out in this policy and ensure that the policy remains up to date with technological changes. The Designated Safeguarding Lead will consider the record of IT incidents and logs of internet activity as part of the ongoing monitoring of safeguarding procedures to consider whether existing practices within the School are adequate.

Consideration of the efficiency of the School's online safety procedures and the education of pupils about keeping safe online will be included in the Governors' annual review of safeguarding.

# Pupil Acceptable Usage Policy

This policy applies to all Pupils at Shrewsbury School and sets down the standards which pupils are required to observe in the use of the IT network, email, internet and other areas covered by this policy.

**It is the responsibility of all pupils 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.

This policy applies to the use of all computing and communications devices, network hardware and software and services and applications associated with the including:

- the internet
- email
- mobile phones and smartphones
- desktops, laptops, netbooks, tablets / phablets
- personal music players
- devices with the capability for recording and / or storing still or moving images
- social networking, micro blogging and other interactive web sites
- instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards
- webcams, video hosting sites (such as YouTube)
- gaming sites
- Virtual Learning Environments such as Firefly
- Interactive boards, Display screens and other projection equipment
- other photographic or electronic equipment e.g. GoPro devices.

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
- Email
- Security
- Copyright
- Social Media
- Use of Technology in Classrooms
- Audio and Visual

# Pupil Acceptable Usage Policy

**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.**

**Safe use of IT**

We want pupils to enjoy using IT and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.

The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. Pupils are educated about the importance of safe and responsible use of ICT to help them to protect themselves and others online.

Pupils may find the following resources helpful in keeping themselves safe online:

http://www.thinkuknow.co.uk/
http://www.childnet.com/
http://www.childline.org.uk/Pages/Home.aspx

Please see the School's Online Safety Policy for further information about the School's online safety strategy.

**Working hours**

The school day is defined as:

- Monday to Friday:
  - 07:00 – 11:10
  - 11:35 – 13:00
  - 14:00 – 17:00
  - 19:15 – 21:00
- Saturday:
  - 07:00 – 11:10
  - 11:35 – 13:00

Pupil relaxed filtering applies at:

- Lunchtime:
  - Monday - Friday 13:00-14:00
- Morning Break:
  - Monday – Saturday 11:10 – 11:35
- Evening:
  - Monday – Friday 21:00 – 23:00 **
- Weekend:
  - Saturday 13:00 – 23:00
  - Sunday 07:00 – 23:00

Evening rules for lights out (no internet access)

| | |
|---|---|
| Third Form | 21:30 |
| Fourth Form | 21:45 |
| Fifth Form | 22:15 |
| Lower Sixth | 22:45 |
| Upper Sixth | 23:30 |

(there is an extension of 15-30 minutes for year groups on Saturday evenings)

# Pupil Acceptable Usage Policy

## Internet

Use of the Internet by all pupils 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, pupils 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 use your Internet access for School related purposes only to research relevant topics and obtain useful School related information.

Access to the Internet is available in the Library, and personal devices until various times; 23:00 hrs being the latest for pupils. This is to be used for genuine research purposes and School related enquiries during school hours.

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.

You must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of the internet in this way is a serious breach of discipline and may constitute a serious criminal offence.

Where possible, pupils should schedule resources-intensive operations such as large file transfers, video downloads, mass emailing and the like for off-peak times. Pupils should adhere to the weekly (Monday-Friday) fair usage download limit of 12Gb.

Any file, including emails, that is uploaded or downloaded must be scanned for viruses before it is run or accessed. This should be done automatically, so pupils must check that their anti-virus 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 discipline 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 pupil may use School facilities knowingly to download or distribute pirated (illegal and unlicensed) software or data.
- No pupil may use the School's network facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the security of themselves or other pupils or staff. **This includes downloading, installing or attempting to use VPN software.**
- No pupil may use the School's network to deliberately propagate any virus, worm, Trojan horse, or trap-door programme code.
- Pupils must not share logon credentials or use school credentials other than those issued to them, even with the agreement or collusion of a third party.

Pupils are specifically prohibited from downloading any software without the express permission of the IT department.

# Pupil Acceptable Usage Policy

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

The School's monitoring system (SmoothGuardian) records (for each and every pupil) each web site visit, each chat-room and each file transfer into and out of its internal networks. **No pupil 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. The Designated Safeguarding Lead will be informed should any such use give rise to safeguarding concerns.

Pupils 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.

Pupils must not use video messaging software to communicate with other pupils. Any use of video messaging software should adhere to common decency rules.

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

It is acknowledged that certain pupils may require, during the normal course of their studies, access to certain sites that may normally be blocked. It is possible to make exceptions in these cases to allow legitimate access, by contacting the IT department; please note that a member of staff may be required to confirm your requirements before access is granted.

Internet access is extended after (and before) working hours, in that the category restrictions are relaxed. For example access to Hotmail, yahoo, Facebook etc. is allowed.

Access to Social Networking sites is only permitted outside of normal School Hours. Accessing Social Networking sites is strictly forbidden during TopSchools. See separate section on Social media below.

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 pupil who attempts to disable, defeat or circumvent any School security facility will be subject to immediate 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 PUPIL WILL BE HELD ACCOUNTABLE FOR ANY BREACHES OF SECURITY OR CONFIDENTIALITY.

Connections to the Internet using a mobile electronic device is permitted providing the permission of the pupil's Housemaster or Housemistress has been sought in advance.

Pupil ID and passwords help maintain individual accountability for Internet resource usage. Any pupil who obtains a password or ID for an Internet resource must keep that password confidential.

Shrewsbury School's policy prohibits the sharing of pupil 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 or the School Librarian.

## Email

Pupils need to be aware that email 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 email as in these other forms of communication.

The definition of Email covers:

i. Electronic Mail services within Shrewsbury Local Area Network (internal email).

ii. Electronic Mail sent through the Internet to other organisations / individuals (external email).

The School provides an email system to support its academic activities and access to email facilities for all pupils is granted on this basis. In addition at specified times and locations pupils may access the facilities for personal activities including communication and recreational use. Pupils are reminded that email 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 email, it is expected that the content meets the standards of professionalism which Shrewsbury School expects of its pupils.

It is not permitted for pupils to send or search for any inappropriate emails, which contain offensive material or would infringe the School's code of conduct. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Do not use aggressive, abusive or deliberately anti- social language. Never email hastily or out of anger.

Use of personal email must not detrimentally affect the duties of other pupils or disrupt the system, and / or harm the School's image or reputation. Pupils 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 email (i.e. Hotmail or Yahoo mail) is permitted for pupils only outside of normal school hours. Be aware that this mail is insecure and may present a security threat.

Pupils must use School email accounts for any email communication with staff. Communication either from a personal email account or to a member of staff's personal email account is not permitted.

Pupils are reminded that they are responsible for their own email housekeeping. Unwanted email should be deleted. If pupils are unsure how to achieve this, guidelines are available from the IT department.

Pupils should not give their external email 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.

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

Pupils should not allow other pupils to use their network login. Pupils should not impersonate other users or use their credentials to access the school network or services via any school or personally owned device. Do not leave your PC logged on to the network.

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 antivirus software is set up to regularly scan each PC for viruses. If pupils notice that their anti-virus software is not running or scanning, they should immediately report the fact to the IT Department.

It is extremely common for a virus to propagate itself via an email attachment. Commonly the attachment will be an executable file (with .exe, .vbs suffix). If there is any doubt as to the authenticity of an email 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 email could be received from a known and trusted source. Pupils 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 your Housemaster / Housemistress, Tutor or the IT department.

The use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while pupils are on School premises or otherwise in the care of the School is discouraged, as pupils are unable to benefit from the School's filtering and anti-virus software. Pupils accessing the internet outside the School's network whilst on School premises or otherwise in the care of the School do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour.

The use of location services represents a risk to the personal safety of pupils and to School security. The use of any website or application, whether on a School or personal device, with the capability of identifying the user's location while you are on School premises or otherwise in the care of the School is discouraged

## 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.

## Social Media

**Social Media** relates to any medium used for social interaction by pupils with other individuals and organisations electronically.

### Core Principles for the use of Social Media

1. The use of Social Media must be responsible, respectful and legal. Posts must never include content that is abusive or that may cause offence to individuals or groups of society.
2. The use of social media must not bring Shrewsbury School into disrepute.
3. Remember that what goes online, stays online. Once you post something on a social media site you acknowledge that this is now shared in a public forum, regardless of any privacy settings.
4. **Social media must not be used by students to contact individual staff members.**
5. Any errors, inaccuracies or other inappropriate content which is posted on School Social Media must be acknowledged and corrected immediately.
6. Use of the school ICT facilities must be in accordance with the remainder of this Acceptable Usage Policy and other legislation that may from time to time be in force.

### Student use of Social Media in School

1. Students are taught how to use social media creatively, respectfully and, above all, safely. This is embedded into the school curriculum and is revisited at various stages in the school to enable age-appropriate discussions of the need for e-safety to take place.
2. Students should consider three areas when using social media - Conduct; Content and Contact.
    a) **Conduct** - Students should present themselves online in a manner which demonstrates respect to the audience; A student's conduct online should give a good representation of themselves to the audience. Students should ask whether they would like to read the same kind of comments posted about themselves in a public forum. All comments should therefore be positive and constructive.
    b) **Content** - If a student is not sure whether the content of their post is appropriate for a public audience, then they should find a more suitable medium to share their comment.
    c) **Contact** - Students should be aware of the need to keep their personal contact details private. They should carefully consider the possible consequences of revealing their personal information in a public forum.
3. Students should be aware of the fact that they can talk to a parent or a member of staff at school if they see something online that makes them uncomfortable or causes them concern.

# Pupil Acceptable Usage Policy

## Use of Technology in School

This section is to be read in conjunction with the remainder of this Acceptable Usage Policy, the Pupil Behaviour Policy, the Anti-Bullying Policy, the Yellow Card and the Child Protection and Safeguarding Policy and Procedures document.

"Technology" means mobile electronic devices including, but not limited to, mobile phones, smartphones, tablets, laptops and MP3 players.

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.**

Mobile telephones should be switched off or in 'silent mode' and out of plain site when in classrooms unless instructed otherwise by a member of staff.

Pupils must not communicate with staff using a mobile phone (or other mobile electronic device) except when this is expressly permitted by a member of staff, for example when necessary during an educational visit. Any such permitted communications should be brief and courteous.

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

Use of technology of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not pupils are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the Anti-bullying Policy and Pupil Behaviour Policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the Child Protection and Safeguarding Policy and Procedures).

Pupils who use technology inappropriately should expect the privilege to be removed and the device to be confiscated for a period of time. Devices may be searched in appropriate circumstances (see the Conducting a Search and Confiscation Policy). Additional sanctions may be considered in light of any other possible contraventions of related School policies.

## Audio and Visual

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.

Using photographic or audio material of any kind to bully, harass or intimidate others will not be

tolerated and will constitute a serious breach of discipline. 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 websites 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.

The posting of images or audio which in the reasonable opinion of the [• Headmaster] is considered to be offensive or which brings the school into disrepute on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image or audio was posted using School or personal facilities.

**Youth Produced Sexual imagery (YPSI) previously referred to as Sexting**

Youth Produced Sexual imagery means the taking and sending or posting of images or videos of a sexual or indecent nature, usually through mobile picture messages or webcams over the internet. YPSI is strictly prohibited, whether or not a pupil is in the care of the School at the time the image is recorded and / or shared. YPSI may also be a criminal offence, even if the picture is taken and shared with the permission of the person in the image.

Pupils should remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others. Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

The School will treat incidences of YPSI (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's Child Protection and Safeguarding Policy and Procedures).