



William Shrewsbury Primary School

Acceptable Use Policy for Internet and Computing

'to inspire a love of learning'

The use of the internet is used by schools habitually. It would be difficult to guarantee restriction of pupils to unwanted internet material and with this in mind the school subscribes to a server which offers protected access, namely, Research Machine's "Netsweeper" which monitors what can be accessed by schools. We also have local management of access through Future Clouds. FC works unobtrusively, monitoring what each user on each device is doing. If there is any inappropriate activity a snapshot of the screen is taken and stored in a log which can be used as evidence. This reduces the likelihood of inappropriate action taking place. As the result of recent Ofsted research shows, learners expect that we will provide them with safe provision.

A school 'Safety Policy' has been produced which supports this policy and has been endorsed by staff and governors.

William Shrewsbury encourages use by pupils of the rich information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our pupils will be entering.

Access to on-line resources will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people throughout the world. The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages.

In order to match electronic resources as closely as possible to the National and school curriculum, teachers review and evaluate resources in order to offer experience of the most up to date technological equipment wherever possible. Alongside this they incorporate Learning Resources containing materials appropriate to age range and ability.

We can protect our children against access to unsuitable material by:

- Continuing to use Netsweeper.
- Accessing sites which have been particularly set up for schools, e.g. Google Schools, Bug Club, Espresso, and Education City.
- Every new term starts with an E-Safety scheme of work in every year group, children are reminded throughout the term whilst using other websites too.
- Providing only supervised access to the Internet.
- Using Hector's world in KS1 and the Foundation Stage, which is a tool for children to block the screen very quickly if they find inappropriate material.
- Common Sense Media Digital Literacy Plans are used throughout school.
- Internet safety week is incorporated into the curriculum along with e-safety assemblies where children are reminded of how to be safe and where to find the appropriate buttons to report unsafe material.
- E-Safety drama production for Years 4, 5 and 6 takes place every academic year. Followed by a workshop and parent assembly. Teachers are also given extra material to continue with safety after this production.
- Children are taught E-safety through PSHE also - please refer to this policy and PSHE schemes of work.
- FC is used in school to further protect children and staff.

- Our children should realise that not all material on the internet is acceptable and we should educate them to make the correct choices should they unwittingly find materials of this kind.

Reminding Parents about E-safety

Annually, at William Shrewsbury, parents are invited to the 'Meet The Teacher' meetings which provide ESafety advice for parents and introduces them to our curriculum content.

Once a year, parents are invited in to watch the final show created with POPUK - where children learn and perform songs about staying safe online.

Parents can also access E-Safety information on the school's website. Newsletters and information leaflets are sent out when needed along with termly newsletter reminders.

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to their teachers and line managers.

Guidelines for Use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite - never send or encourage others to send abusive messages.
2. Use appropriate language - users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy - do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
5. Password - do not reveal your password to anyone. If you think someone has learned your password then contact the ICT technician.
6. Electronic mail - Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
7. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
8. Staff or students finding unsuitable websites through the school network should report the web address to the ICT technician.
9. Do not introduce "pen drives" into the network from unknown sources.

10. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity. All sites visited leave evidence in the county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
11. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.
12. Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
13. Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
14. Disruptions - do not use the network in any way that would disrupt use of the network by others.
15. Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety is deemed unacceptable.
16. Receiving, sending or publishing material that violates copyright law, Data Protection Act or breaching the security this act requires for personal data is unacceptable.
17. User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere is not acceptable.
18. Do not use internet sites that are not related to the curriculum or your job description within working hours.
19. All of the above should be taken into account when using school bought equipment, e.g. cameras, laptops etc.
20. **All staff must read and sign responsible use forms. All staff and children accept the AUP termly which appears on screen.**

The school expects that staff will investigate possibilities and blend use of such information, as appropriate, within the curriculum and that staff will provide guidance and instruction to pupils in the appropriate use of such resources. Staff should consult the Computing Lead for advice on content, training and appropriate teaching levels consistent with the school's ICT programme of study.

Independent pupil use of telecommunications and electronic information resources is not advised. Parents will be asked to complete permissions and agreement forms before their child may publish information on the Internet or access electronic forms of communication.

Social Networking

Social networking sites are blocked; however Youtube is currently accessible on the understanding that students should use it responsibly without impacting on learning. YouTube for schools is accessible in classrooms. This not only includes students but staff also.

Mobile phones

Students are not permitted to have mobile phones on site without permission from a member of staff. Anyone seen using a mobile phone will have it confiscated for at least the remainder of the day.

Staff in school should keep their mobile phones on silent or switched off and always out of sight of children unless deemed necessary (school trips/emergency).

All other web based technology

There are various other technologies involved in teaching and learning which may involve the sharing, uploading and downloading of all media files, for example: webcams, microphones, digital cameras, video recorders, iPads etc. Staff and pupils alike are trusted to use the equipment appropriately and with suitable permission, in accordance with data protection.

Access to the internet offers both students and teachers vast, diverse and unique resources. Unfortunately, as there is the possibility that students will encounter inappropriate material, the school has taken and will continue to take all reasonable precautions to ensure that students access appropriate material only. However, it is not possible to guarantee that a student will never come across unsuitable material while using a school networked computer. The school however, can not accept liability if such material is accessed nor for any consequences resulting from internet access.

William Shrewsbury Primary School

E-mail and Internet Use Good Practice

Rules for ICT Use

*We use the school computers and Internet connection for learning.
These rules will help us to be fair to others and keep everyone safe.*

- I will ask permission before entering any Web site, unless my teacher has already approved that site.
- On a network, I will use only my own login and password, which I will keep secret.
- I will not look at, change or delete other people's files.
- I will not bring external storage devices to use in school without permission.
- I will only use the computers for school work and coursework.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit.