The Weaverham
Primary Academy
Inspire, Nurture, Flourish

Online Safety Policy

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Developing effective practice in Internet use for teaching and learning is essential as the quantity of information is often overwhelming. Staff will guide pupils to appropriate websites, or teach search skills. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

We will ensure that Internet access will be

- planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. To protect the pupils as much as possible the following safeguards are in place:

Filtering

- The computers are located in the classrooms where children are seldom left unattended.

- Pupils are taught what to do if they experience material that they find distasteful, uncomfortable or threatening. In such circumstances they close the page and report the incident immediately to the teacher.

More often, pupils will be judging reasonable material but will need to select relevant sections. Pupils will be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information as well as comparing web material with other sources.

How will information systems security be maintained?

The server can be accessed through the intranet at school. Each child has a file within their year group. These can be used to "back up" work created on the learning platform but can only be accessed from school.

- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured. Portable media may not used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail e.g. videos from YouTube.
- Files held on the school's network will be monitored by class teachers during lesson time.
- The ICT co-ordinator / network manager will review system capacity regularly.

How will e-mail be managed?

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits for example communication between schools from different localities and even continents can be created. However it is vital that safety measures are put in place as un-regulated e-mail can provide routes to pupils that bypass the traditional school boundarie

In the school context, e-mail is not considered private and so we reserve the right to monitor e-mail in order to maintain the safety of pupils

- Whole-class e-mail addresses will be used
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils will be taught they must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

How will published content be managed?

The school website is an excellent medium for communicating with families both current and prospective as it can celebrate pupils' work, promote the school and publish resources for projects. However publication of information should be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published, e.g. photographs of pupils will never be named.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Can pupil's images or work be published?

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified (i.e. never named).
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs, where no names will be used.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

How will social networking and personal publishing be managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: blogs, wikis, MySpace, Bebo, Piczo, Facebook, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others.

- The schools firewall will block or filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be taught not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

How will videoconferencing be managed?

At present we do not have the facilities for videoconferencing.

How will e-safety complaints be handled?

We value the safety of all members of our school community in whatever context they may be working and recognise that e safety is an important element of this.

Prompt action will be required if a complaint is made regarding any member of the community and the facts of the case will need to be established.

- A minor transgression of the rules may be dealt with by the teacher.
- Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator. Advice on dealing with illegal use could be discussed with the local Police Officer connected to school.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions within the school discipline policy include
- Informing parents or carers;
- Removal of Internet or computer access for a period.

How is the policy introduced to pupils?

- Online-Safety rules will be posted in rooms with Internet access and agreed by class teachers in a staff meeting and introduced by the school council.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use, particularly to those pupils new to the E Learning Platform.
- Instruction in responsible and safe use should precede Internet access.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. The School e-Safety Policy will only be effective if all staff subscribe to its values and methods and so this policy has been developed with the full agreement of all concerned.

- All staff will be given the School Online-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home through recommended websites specifically on safe internet use, via the school website.

- Parents' attention will be drawn to the school's e-Safety Policy at a meeting to introduce the e-learning platform, in newsletters, the school prospectus and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged.

Appendix

Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of electronic communications.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;
- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Policy reviewed: September 2019
Date of next review: September 2021