Online Safety Policy

1 Policy Statement

Worthington Primary School recognises that the Internet is an essential element in 21st century life for education, business and social interaction. The school therefore has a duty to provide students with quality Internet access as part of their learning experience.

The Internet allows access to a vast array of information resources, readily providing answers to questions that may arise across the curriculum. It also provides a wealth of engaging games and activities that can enhance children's learning experiences. Furthermore, it can facilitate educational and cultural exchange through the use of e-mail and forums. We aim to encourage pupils to use the rich resources available on the Internet to enhance their learning and understanding of world.

We recognise that in order to do so the children must develop appropriate skills to analyse and evaluate such resources. These skills will be fundamental in both the children's future schooling and in the society our pupils will be entering. As such our staff will use the Internet as a research tool in all areas of the curriculum and will provide guidance and instruction to pupils in the appropriate use of such resources.

The unregulated nature of the Internet raises unique concerns that must be addressed if the children are to use the Internet safely. This policy outlines the procedures in place in school to ensure that staff and pupils have controlled safe access to the Internet.

The school believes that the benefits to pupils from controlled access to information resources and increased opportunities for collaboration exceed the disadvantages. If children are to succeed in today's information rich environment they need to be aware of the Internet's potential dangers and how to deal with them.

This E-safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

The 4 key categories of risk

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

E-safety in the Curriculum

The school provides opportunities within a range of curriculum areas to teach about e-safety.

Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.

The teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Pupils know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member.

2. Controlled Internet Access in School

All internet activity within school is monitored and filtered through Trafford's system. In school we also have and IT provider, Infinity computing. They are responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the headteacher, computing lead, DSL and relevant staff. for investigation and action.

At Worthington, we also use Smoothwall to keep children safe which enables school to monitor usage and be notified immediately of any breaches of internet safety.

On-line services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials would be chosen to be consistent with national policies, supporting and enriching the curriculum while considering the varied teaching needs, learning styles, abilities and developmental levels of the pupils.

Free Internet access - because it may lead to any publicly available site in the world - would open our classrooms to electronic information resources which have not necessarily been selected by teachers. Therefore, the children will have 'controlled access' to the Internet. This will be achieved in a number of ways:

- Children will only be allowed to access the Internet in the presence of a trained member of staff;
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use;
- All children and staff will be fully aware of the school's 'Rules for Responsible Internet Use' and will have signed to say that they will adhere to them at all times;
- When using search engines and websites with the children, staff will first have accessed the relevant pages themselves to check for inappropriate material;

- Broadband Internet access will be via Trafford's Intranet and will be controlled by its 'web-nanny';
- E-mail will usually only take place within school. Where external e-mail is necessary (for example educational and cultural exchange) it will take place only to approved e-mail addresses and in supervised lesson time;
- All external 'chat' based services will be blocked and it will be forbidden to attempt to access them.
- As part of the ICT (Information and Communications Technology), PSHCE (Personal, Social, Health and Citizenship Education) and SEAL (Social and Emotional Aspects of Learning) curriculum pupils will be taught about a range of issues related to internet safety.
- All staff will be fully aware of the procedures to be carried out if inappropriate material is accessed.
- Posters outlining the Rules for Responsible Internet use will be displayed in all rooms containing a computer.
- The school will work in partnership with parents, the LEA, DfES and our Internet Service Provider to ensure systems to protect pupils are regularly reviewed and improved.

3 Rules for Responsible Internet Use for Pupils

Pupils are responsible for good behaviour on the Internet just as they are responsible for their behaviour in the classroom or playground. General school rules apply.

The Internet is provided for the pupils to conduct research and communicate with others. Parents' permission is required.
Pupils should remember that access is a privilege not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards.

Computer storage and portable storage will be treated like pupils' classroom drawers. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.

The following activities are not permitted:

1. Sending or displaying offensive messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others.
4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws - therefore a teacher must be consulted before printing or downloading of material takes place.
6. Using others' logons and passwords.
7. Trespassing in others' folders, work or files.
8. Intentionally wasting limited resources.
9. Using portable media (such as CDs and memory sticks) on the school network without specific permission and a virus check.

4 Rules for Responsible Internet use for Teachers and other Adults

1. Do not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.

2. Do not give personal addresses, telephone/fax numbers of: -
   a. any adult working at the school;
   b. any students at the school.

3. Use of names of students, or photographs of students will require written permission from parents

4. Do not download, use or upload any copyright material. Always seek permission from the owner, before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material.

5. Under no circumstances should you view, upload or download any material, which is likely to be unsuitable for children. This applies to any material with violent, dangerous, sexual or inappropriate content.

6. Always respect the privacy of files of other users. Do not enter the file areas of other staff without their express permission.

7. Be polite and appreciate that other users may have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Do not state anything, which could be interpreted as libel or is potentially offensive to anybody.

8. Report any incident, which breaches the Acceptable Use Policy immediately to the ICT co-coordinator or Headteacher.

9. Users should not expect that files stored on servers or disks would always be private.

10. Any information retained electronically i.e. pupil records and assessments will be password protected and held securely.

5. Mobile Technologies

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom.

These are not to be used at any time whilst children are present and only in the staffroom or school offices.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Managing email

The use of email within school is an essential means of communication for staff. Pupils currently do not access individual email accounts within.

Staff must use the school's approved email system for any school business.

Staff must immediately inform the Head teacher, computing lead or It provider if they receive an

inappropriate of offensive email.

6 Procedures

If it is found that the 'Rules for Responsible Internet Use' have been deliberately breached the following sanctions will apply:

1. A temporary or permanent ban on Internet use will be applied.
2. Additional disciplinary action may be added in line with the school's existing behaviour policy.

When applicable, police or local authorities may be involved.

Any breaches of these rules will be dealt with by the Headteacher.

If inappropriate material is inadvertently accessed the following procedures will apply:

1. It will be calmly explained to the child that they have accessed material that the school does not wish them to view. It will be immediately removed from their sight. If necessary a member of staff may ask how the child came to access the material.
2. The member of staff supervising will note the web address of the inappropriate material and keyword used to access it. This will be immediately passed to the ICT coordinator who will update the electronic filtering software to ensure it cannot be accessed again.
3. The Headteacher will be informed. If necessary, elements of the Acceptable Use of the Internet Policy may be reviewed.

7. Virtual Learning Environments

At Worthington we believe that use of the latest technologies can enrich children's learning experiences. Virtual Learning Environments (VLEs) can play a key role in ensuring that our children's use of ICT better reflects the nature of ICT usage in the wider world. This can be achieved by:

1. Allowing children to directly access digital learning resources recommended by their peers and teachers.
2. Enabling them to take part in educational discussion forums.
3. Allowing teachers to set and receive homework tasks digitally.
4. Giving children their own customisable online space.
5. Providing children with a safe environment in which to communicate.

To ensure that every child is able to safely benefit from these features each child is provided with a personal logon and password. It is their responsibility to not disclose this information to anyone except their parent or carer. Activity within the learning environment is closely monitored by the class teacher and ICT coordinator and any inappropriate behaviour will be dealt with in line with the procedures outlined in this document.
Pupils need to realise that these rules and procedures also apply to their use of the VLE outside of school. Incidents of misuse will be dealt with in exactly the same manner as if the incident had taken place in school.

8. School Website

The school website plays an important role in enhancing links with the wider school community and can be a motivating force for the children.
In order to achieve this, pictures of the children at work and play and examples of the children's work may be used. All content on the website is screened by the class teachers, ICT coordinator and Headteacher. We also ensure that children's names never accompany their photograph and

that they are happy for their work to appear online.

9. Cyberbullying

Cyberbullying can be defined as the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.
Pupils are responsible for good behaviour in their use of ICT at home just as they are responsible for their usage of ICT and behaviour in school. General school rules apply.
Mobile phones are not permitted in school unless there is a letter from a parent/carer to say that the phone is essential for the safety of their child during their journey to or from school. If this is the case, the phone should be passed to the class teacher each morning to look after during the school day.
In dealing with incidents involving the receipt of messages or content that they do not feel comfortable with, pupils will be encouraged to:

1. Immediately inform an adult that they trust.
2. Print off, or store, the message as evidence.
3. Inform the school as soon as possible.

10. Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

At Worthington we recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

At Worthington we will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust.

11. Disclaimer

In common with other media such as magazines, TV, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, it should be noted that due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Updated: November 2024
Review due: November 2025

Policy ratified at Full Board of Governors, in line with the safeguarding policy