USWORTH COLLIERY
PRIMARY SCHOOL

E Safety Policy

Designated members of staff: Alison Forster.

Chair of Governors: Alison Logan

What is an e-safety policy?

The E-Safety Policy is part of the School Development Plan and relates to others including those for ICT, Anti-Bullying and Safeguarding. This E-Safety Policy replaces the previous policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole. E-safety encompasses, not only Internet technologies, but also electronic communications such as smartphones, tablets and other wireless devices.

Why have an e-safety policy?

It highlights the need to educate children and staff about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. Anyone can send messages, discuss ideas and publish material with limited restriction. These features make it an invaluable resource used by millions of people every day. However, much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism – access to which would be more restricted elsewhere. Pupils must also learn that publishing information could compromise their security and that of others.

Why is use of the Internet important in supporting learning?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

How does the Internet benefit education?

Benefits of using the Internet include:

➢ Access to world-wide resources
➢ Educational and cultural exchanges between pupils world-wide
➢ Cultural, vocational, social and leisure use in all aspects of everyday life.
➢ Access to experts in many fields for staff and pupils
➢ Staff professional development through access to national developments, educational materials and good curriculum practice
➢ l developments, educational materials and effective curriculum practice
➢ Communication with support services, professional associations and colleagues
➢ Improved access to technical support including remote management of networks and automatic system updates
➢ Exchange of curriculum and administration data with the Local Authority and DfE
➢ Access to learning wherever and whenever convenient

How will Internet use enhance learning?

➢ School Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils
➢ Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
➢ Pupils will be educated in the effective use of the Internet in research, including exploring the validity of different sources
➢ Pupils will be shown how to publish and present information to a wider audience
➢ Internet access will be planned to enrich and extend learning activities as an integrated aspect of the curriculum

- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity
- Pupils will use the internet discerningly to answer key questions and follow lines of enquiry
- Pupils will select suitable websites and will be encouraged to take responsibility for their own internet access

How will pupils learn to evaluate Internet content?
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law
- Pupils will be taught the importance of cross-checking information before accepting its accuracy and to question the credibility of the information
- Pupils will be taught how websites are ranked when using search engines and how to avoid the bias and manipulation that is possible in the way results are presented
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or other in-house reporting services.
- Staff will be made aware of how to report unpleasant Internet content; informing the ICT Coordinator or a member of SMT directly who will contact BT and/or Omnicom.
- Pupils will be informed that checks are made on files held on the system as part of the school's work with the Internet Service Provider to ensure that pupils are protected
- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on television.

How will Internet Access be managed?
- School ICT security and filtering systems provided and managed by Omnicom will be regularly reviewed and upgraded.
- Securus will be used to monitor online activity.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.

How will Removable Media and Hand-Held Devices be managed?
Removable media refers to anything that can be used for taking electronic information out of school. This includes USB sticks; memory cards etc. Also, many consumer electronic gadgets such as smartphones and tablets (iPads) can be used for removable data storage.

Rules about the use of Removable Media of Hand-Held Devices
- Staff must ensure that portable storage devices are encrypted if they include sensitive, confidential or personally identifiable information. All staff members have been issued with encrypted USB pens and these must be used to store any data or information of any kind relating to their pupils. Good practice dictates that all data which refers to individuals or contains sensitive information of any kind should be encrypted.
- Staff must obtain approval from a member of the Senior Management Team or the Head Teacher before creating, moving or copying information, files, folders etc… onto a portable storage device.
- Staff should ensure that portable devices are stored securely when left unattended (including the locking of screens).
- Staff should ensure that portable technology such as the iPads are password protected.
- Staff should ensure that devices taken off-site should not be left unattended in public places or at an individual's home address.
- To avoid total loss of data, users are to ensure that information stored on the portable devices is 'backed-up' and held in the appropriate place on the school network.
- If a portable storage device or hand-held device is lost, stolen or mislaid staff must report it immediately to the Head Teacher and, where appropriate, the ICT Engineer.
- Staff should only use equipment that has been purchased or approved by the school.

➢ Staff are responsible for ensuring that visitors or contractors who bring their own devices into school (to give a presentation for example) are supervised at all times while the device is connected to school equipment. This should only occur if unavoidable and needs to be connected in consultation with our technical support service (Omnicom).

E-mail

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects. However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, e-mail is not considered private and is monitored by staff, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

➢ Pupils may only use approved e-mail accounts on the school system (Office 365) that have the appropriate educational restrictions applied.
➢ Pupils must immediately tell a member of staff if they receive offensive or inappropriate content.
➢ In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
➢ Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
➢ If appropriate, the school should consider how e-mail from pupils to external bodies is presented and controlled. E-mail sent to an external organization is written carefully and authorized before sending.
➢ The sending of abusive or inappropriate email messages is forbidden.

Social Networking and E-Communication

Conferencing applications offering the instantaneous exchange of content between users have great potential for education and provide a basis for pupils' understanding of global citizenship as they encounter different societies and cultures. Further information is provided in the Twitter/X Policy.

➢ Pupils will not be allowed access to public or unregulated social media.
➢ They will be closely supervised during well-planned activities and the importance of using technology safely and sensibly clearly emphasised.
➢ Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
➢ Pupils will be advised to use nicknames and avatars when using social networking sites.
➢ Newsgroups will not be made available unless a specific educational requirement for their use has been demonstrated.
➢ Risk assessment will be carried out before pupils are allowed to use emerging technologies in school.
➢ Pupils will use only moderated and carefully selected E-Communication sites, for example, Seesaw.
➢ Pupils and parents will be advised on how to safely utilise social networking spaces outside school.
➢ Mobile phones will not be used during lessons or school session times. Staff are provided with a locker for the storage of mobile phones as they are not permitted in classrooms or other areas of the school where there are pupils.

Publishing on the Web

A Website is the ideal way to promote our school, celebrate good work, to inform parents/carers and to publish resources useful for homework. It is important that the Website reflects our ethos, the information is correct, and that pupils and staff are protected.

- ➢ Staff or pupil personal contact information will not generally be published.
- ➢ Personal data will be recorded, processed, transferred and made available according to GDPR.
- ➢ Photographs that include pupils will be carefully selected so that individual pupils without the appropriate consent cannot be identified or their image misused.
- ➢ Group photographs will not have name lists attached.
- ➢ Pupils' full names will not be used anywhere on a school website or on other online spaces, particularly in association with photographs.
- ➢ Written permission from parents or carers will be obtained before photographs of pupils are published on the website or other online spaces and parents/carers will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- ➢ Work can only be published with the permission of the pupil and parents/carers.
- ➢ Work must be the author's own and credit any other work included.
- ➢ The Head Teacher will delegate responsibility to an identified member of staff to ensure that content is correct and quality of presentation is maintained.
- ➢ The point of contact on the Website will be the school's address and telephone number.
- ➢ Home information or individual e-mail identities will not be published.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to GDPR.

Managing videoconferencing & webcam use
The following guidelines must be adhered to if using video facilities in school:

- ➢ Pupils must ask permission from the supervising teacher before using cameras.
- ➢ Camera use will be appropriately adapted to the pupils' age.
- ➢ Video conferencing should use the educational broadband network to ensure quality of service and security.

Managing emerging technologies
- ➢ Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- ➢ SMT should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- ➢ Mobile phones will not be used during lessons or within formal school time. The sending of abusive or inappropriate text messages is forbidden.
- ➢ The use by pupils of mobile technology, such as iPads, will be monitored.
- ➢ Staff will agree to terms and conditions before access to school technology is granted (see Appendix III, IV & V).

Managing use of Artificial Intelligence

We recognise that Artificial Intelligence (AI) technologies can support learning, teaching, assessment, administration and school operations when used safely, ethically and responsibly.

The school expects that staff:

- ➢ Use AI only to support professional duties, such as planning, resource development, feedback and administrative tasks.
- ➢ Only AI systems approved by Usworth Colliery Primary School may be used for work-related purposes.

- Use school-provided or school-approved AI accounts where these are available (Microsoft Copilot as part of Office365).
- Support, not replace, professional judgement. All final decisions, especially those affecting pupils, staff or families, must be made by a human.
- Are professionally accountable for all AI-assisted outputs and must critically evaluate, fact-check and review content before use to ensure that it is accurate, appropriate and suitable for a primary school context.
- Never enter personal, sensitive or confidential data into AI systems.
- Ensure that any data shared is anonymised and complies with UK GDPR and data protection legislation.
- Take care to protect copyright and intellectual property, including learner work, and avoid unauthorised use of AI-generated material.
- Are aware that AI systems may produce biased, inaccurate or discriminatory outputs and must address these risks.
- Should make it clear where AI has supported the creation of professional material where appropriate.

Any AI-related incident, concern or misuse must be reported immediately in accordance with school safeguarding and reporting procedures. Where appropriate, staff will receive training and guidance in the safe and responsible use of AI.

Misuse of AI systems may lead to disciplinary action, in line with school policies.

The school expects that pupils:

- Use AI tools only when allowed and supervised by a teacher.
- Use only AI systems approved by the school for learning activities.
- Understand that AI does not always provide correct or reliable information.
- Learn to question, check and discuss AI-generated information with a trusted adult.
- Never share personal information, including names, photographs, addresses or passwords, with AI tools.
- Do not upload images, schoolwork or information about themselves or others without adult permission & support.
- Understand that copying AI-generated work and claiming it as their own is not acceptable.
- Respect copyright and other people's work, including work generated using AI.
- Immediately tell a trusted adult if AI content makes them feel worried, upset or uncomfortable and/or appears unkind, unfair or inappropriate
- Understand that school online safety rules apply when using AI, including when learning at home if it relates to school.
- Learn about AI through age-appropriate lessons, helping them to make safe, responsible and thoughtful choices.
- Are supported to use technology in a healthy and balanced way.

As a school, we aim to promote good practice through multiple methods including displays (appendix VII), online content such as social media and the school website and curriculum content.

How will Internet access be authorised?
It is essential that all staff and pupils are aware of the need for safety when accessing the Internet.
- All staff, including supply staff, classroom assistants and support staff will be provided with the E-Safety Policy and its implications discussed.

- ➢ Visitors using the Internet with pupils must sign an *Acceptable Internet Use Statement for Staff and accept the Staff Code of Conduct* (see Appendix III & V) before using the Internet in school.
- ➢ Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential
- ➢ Rules for Responsible Internet use will be displayed in poster format in all rooms where computers are used (see Appendix VI).
- ➢ The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- ➢ At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- ➢ At Key Stage 2, supervised Internet access will be granted to a whole class or individual pupils.
- ➢ Parents/carers will be asked to sign and return a permission form, which is part of an overall agreement from (see Appendix I).

How will risks be assessed?

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of Internet access.

- ➢ Senior staff, in conjunction with private providers (Omnicom), will ensure that regular checks are made to ensure that filtering methods selected are appropriate, effective and reasonable.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web-based content so the school will work in partnership with parents, the LA, the DFE and private providers (*Omnicom*) to ensure systems are reviewed and improved where possible.

How will E-Safety complaints be handled?

- ➢ Complaints of Internet misuse will be dealt with by a senior member of staff.
- ➢ Any complaints about staff misuse must be referred to the Head Teacher.
- ➢ Pupils & parents will be informed of the complaints procedure policy.
- ➢ Pupils & parents will be informed of consequences for pupils misusing the Internet.
- ➢ Sanctions for irresponsible use will be linked to the school's Behaviour Policy and may involve a pupil being denied Internet access for a specified period.
- ➢ Discussions may be held with the Police to establish procedures for handling potentially illegal issues.
- ➢ Complaints of a Child Protection nature must be dealt with in accordance with school Safeguarding procedures.

How will we enlist the support of parents and carers?

Internet use in the home and beyond is now common. However, not all parents exercise the same level of supervision over their children's Internet use and the sites they access. In order to protect pupils:

- ➢ Parents' and carers' attention will be drawn to the School E-Safety Policy, and other appropriate materials, in newsletters, the school prospectus and on the school website.
- ➢ The school will maintain a list of e-safety resources for parents and carers. (appendix iii)
- ➢

Author: P Arthur
Agreed date: May 2022
Modified: January 2026
Implementation date:
Review Date: Every 3 years

Signed …………………………………………………………. Date ……………………………….
           Head Teacher

Signed …………………………………………………………. Date ……………………………….
           Chair of Governors

Permission / Agreement Signatures

Dear Parent/Carer,

Below are a number of items for which we require your permission or agreement. We would ask that you sign below each item to which you give permission.

Child's Surname:_____ Child's

Forenames:_____

Male ☐   Female   ☐   Date of Birth:_____

Name of parent completing this form:_____

Uniform

I am willing to dress my child in appropriate, accepted uniform which is clearly labelled with my child's name. I have read and understood the Uniform Policy (available on the school website or ask for a copy at the school office).

Signed:_____   Date:_____

Educational Visits

I give permission for my child to be taken out of schools for visits by walking, school mini bus or external coach companies. I will be informed of all school trips via text, emails or a note, but do not need to give consent for each individual trip.

Signed:_____   Date:_____

Library and other school books

I am prepared for my child to borrow a library book or other school books and take full responsibility for any lost or damaged books.

Signed:_____   Date:_____

Internet

I give my child permission to have supervised access to internet services for educational purposes (see E Safety Policy available on the school website or ask for a copy at the school office)

Signed:_____   Date:_____

Useful sites for parents/carers interested in safe internet use at home:

Further information can be found on our E-Safety page:

https://www.usworthcolliery.co.uk/children/e-safety

Useful Websites:

A) Childnet – A range of resources for families and schools – **http://www.childnet.com/**

B) Talk to someone who is trained to help you at – **http://www.bullying.co.uk/**

C) kidshealth.org – A range of resources geared towards keeping children safe online –
 http://kidshealth.org/parent/positive/talk/cyberbullying.html

Usworth Colliery Primary School
Acceptable Internet Use Statement for Staff

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

> ➢ Access must only be made via the authorised account and password, which must not be made available to any other person
> ➢ All Internet use should be appropriate to staff professional activity
> ➢ Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden
> ➢ Sites and materials accessed must be appropriate to work in school; Users will recognize materials that are inappropriate and should expect to have their access removed
> ➢ Users are responsible for communication they send and for contacts made that may result in e-mail being received
> ➢ The normal rules of social interaction apply to any e-communication for school purposes. The remoteness of the recipients must not be used to excuse anti-social behaviour: harassment, intimidation and bullying behaviour
> ➢ The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded
> ➢ Posting anonymous messages and forwarding chain letters is forbidden
> ➢ Copyright of materials and intellectual property rights must be respected
> ➢ Legitimate private interests may be followed, providing school use is not compromised
> ➢ Use for personal financial gain, gambling, political purposes or advertising is forbidden.

Appropriate Use of Artificial Intelligence (AI)

I agree that:

> ➢ I will use only school-approved AI systems for professional purposes.
> ➢ AI will support, not replace, professional judgement.
> ➢ I remain fully accountable for any AI-assisted work I produce or use.
> ➢ All AI outputs will be checked for accuracy, bias and appropriateness.
> ➢ I will not enter personal, sensitive or confidential data into AI systems (in compliance with UK GDPR and the Data Protection law)

Any data breach or concern will be reported immediately.

Staff requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Head Teacher for approval.

Full name … post … … … … … … … … … … … … … …

Signed … date … … … … … … … … … … … … … …

Access granted … … … … … … … … … … … … … … … … … … date … … … … … … … … … … … … … …

Staff Electronic Device Agreement

Make:_____ Model:_____

Serial No._____ Device ID:_____

I acknowledge receiving the above School device and will use it appropriately and in line with the school Acceptable Use Policy and the recent Social Networking Policy which I have signed and agreed to.

With specific relevance to;

- Where it is intended to use social networking sites on mobile devices owned by the school, you should ensure you have received approval from a member of the SMT prior to undertaking such activities.
- Personal use of the internet, including access to social networking sites, will NOT be permitted on school based equipment in use in school either before or after work or during designated lunch periods. Non work related access during work time and whilst on school premises is not permitted.
- Usage of mobile devices at home should not involve any breach of copyright, or promote any financial, commercial, business, or political interests.
- When downloading personal apps, they must firstly be stored in a 'personal folder' and personal Apple IDs should be signed out immediately after use.
- Personal apps not installed by the school should not be accessed whilst on school premises.
- Any personal apps that require a log in must always be logged out before entering school premises.
- Shared devices, which are not solely intended for the use of one individual, should not have personal apps installed nor should they have personal or work email accounts set up on the device.
- Staff should be aware that all <u>internet usage is monitored</u> and stored on the device and should refrain from accessing personal banking accounts or similar for security purposes as they may be accessed by another individual.
- Passcodes set up by the school MUST not be removed or changed without prior permission.
- Mobile devices owned by the school must be brought in to school each day along with chargers and should be made available for random checks and maintenance.
- Only school-approved AI systems are to be used for professional purposes in accordance with UK GDPR and the Data Protection law.

Any damage to the device MUST be reported IMMEDIATELY to the Head teacher, ICT Co-ordinator or the IT Technician.

I understand that the device will remain the property of Usworth Colliery Primary School and that I am solely responsible for it and must return it to the school should my employment at the school terminate.

I agree to the above:

Signed: _____ Print Full Name: _____

Date: _____

### *Staff Code of Conduct*

Reviewed December 2020

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role.

- I understand that school information systems may NOT be used for private purposes whilst on school premises, e.g. accessing personal email accounts and personal internet use.

- I will use the email account that I have been issued with by the school for sending and receiving emails for work related purposes only and no other email accounts on school computers.

- I will only use the internet for work related purposes whilst at school or whilst logged into a school account using a school laptop.

- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.

- I will respect system security and I will NOT disclose any passwords or security information to anyone other than an appropriate system manager.

- I will NOT download or install any software or hardware without prior permission.

- I will NOT plug in any portable storage devices (e.g. memory sticks) without having them scanned by the ICT Engineer prior to use.

- I will ensure that pupil's personal data is kept secure and is used professionally and appropriately within my role in school. I will NOT take pupil's personal data off the school premises without approval by the Headteacher first. I will ONLY store Pupil's personal data on the schools server and NOT on laptops, memory sticks or any other portable devices that are not encrypted.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the school e Safety Coordinator or the Designated Child Protection Coordinator.

- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

- Network access must be made only via the user's authorised account and password, which must NOT be given to any other person.

- I will NOT leave computers/laptops/iPads logged on whilst unattended.

- I will NOT use chat rooms or any other form of social networking site whilst in school and will follow the guideline expressed in the school Acceptable Use Policy whilst at home.

- Use for personal financial gain, gambling, political purposes or advertising is NOT permitted.

The school may exercise its right to monitor and log the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

By clicking 'I Accept' you acknowledge reading and agreeing to comply with the School Acceptable Use Policy, GDPR Policies and the above Staff Code of Conduct and are aware of your responsibilities.

Rules when using the ICT room
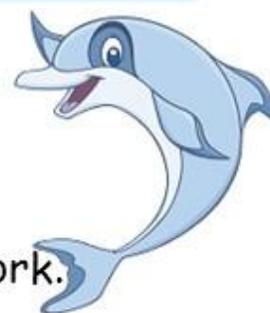
1) I will only use my own Login.

2) I will not open or change other people's work.

3) I will only use school computers for school work and homework.

4) I will not bring in disks or memory sticks from outside school unless I have been given permission.

5) I will ask before using the Internet.

6) I will only use my school email address to message pupils from this school or people my teacher has approved.

7) The messages I send will be polite and appropriate.

8) I will not give any personal details such as my home address, telephone number or home e-mail address or arrange to meet someone unless I have been given permission to do so (e.g. school visit).

9) I will report anything inappropriate that appears on screen or is sent to me.

10) I understand that the school may check my files and the Internet sites that I visit.

CEOP REPORT
ceop.police.uk

✦ Using AI Safely at ✦
Usworth Colliery Primary School

✅ AI can help us to:
- ✓ Learn new things
- ✓ Get ideas and practice skills
- ✓ Support teachers with planning and learning

⚠️ AI is not always right
- ✓ AI can make mistakes
- ✓ AI does not always tell the **truth!**

🛡️ Stay safe when using AI
- ✓ Use only AI tools **that are approved**
- ✓ Ask an adult if you unsure
- ✓ Be kind and respectful 🚫 Don't copy
- 🚫 Personal information   information

🧠 Be smart
- ✓ AI is a tool, not a replacement for thinking
- ✓ You're not sure what to do — **please ask!**

❤️ Remember
We all help keep Usworth Colliery Primary School safe.