Uplands Primary School Online Safety Policy

Date agreed by the Governing body: October 2026

Date for review: October 2027

Introduction

Online safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The school's online safety policy should operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Child Protection, Safeguarding, Home learning, Remote Education, Data Protection and Security.

Our whole school approach to the safe use of computing technologies

Creating a safe computing learning environment includes these main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- Online safety teaching is embedded into the school curriculum and schemes of work
- Responsible technology use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems by:
    - identify and assign roles and responsibilities to manage filtering and monitoring systems
    - review filtering and monitoring provision at least annually
    - block harmful and inappropriate content without unreasonably impacting teaching and learning
    - have effective monitoring strategies in place that meet pupils safeguarding needs (KCSIE 2026 paragraph 142)

The technologies

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information. Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include but are not limited to:

- Internet browsers and search engines
- email
- Instant messaging (often using simple web cams) e.g. WhatsApp, iMessage)
- Web based voice and video calling (e.g. Skype, Facetime, Zoom)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook, Instagram, Snapchat)
- Blogs and Micro-blogs (e.g. X, Threads)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites and livestreaming (e.g. You Tube, Tik Tok, Twitch)
- Homework learning platforms (Seesaw, Mathletics, Spellingshed)
- Music and video downloading (e.g. Apple Music, Spotify)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

- Virtual reality
- Online Video Gaming

Artificial intelligence (AI) tools, including voice assistants and generative AI systems (Amazon Alexa, Google assistant, Siri, Chat GPT, Grok, etc), are treated as online content and information sources. Their use within school is carefully managed and age-appropriate. Pupils are not permitted to use generative AI tools independently. Where AI-enabled tools are used to support learning, this will be under direct staff supervision, with clear guidance provided to pupils about accuracy, bias, misinformation, and safe use. Staff remain responsible for ensuring that any AI-supported content is suitable for pupils and does not expose them to inappropriate material or undermine learning or safeguarding.

School Online Safety Policy

The school's Online Safety Coordinator is also the Computing Manager. They will work in close co-operation with the Headteacher and Senior Leaders; who are the Designated Safeguarding Leads,

Our Online Safety Policy has been written by the school. It has been agreed by the staff and governors.

Online Safety issues are included in the Child Protection, Health and Safety, AntiBullying, Acceptable Use, Social media and Use of Mobile Phones & Digital Photography Policy

The Online Safety Policy will be reviewed on an annual basis.

Teaching and learning

We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At our school, we are committed to teaching pupils to use the technology critically, effectively and appropriately in all aspects of their education.

Internet access at school

Use of the Internet by pupils

Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the Internet, and fixed computers with Internet access are carefully located so that screens can be seen at all times by all who pass by. Laptops and ipads are only used when supervised by a member of staff. During lessons, staff regularly circulate to monitor internet use. The school Internet access will block harmful and inappropriate content without unreasonably impacting teaching and learning by including filtering appropriate to the age of pupils; provided by SchoolsBroadband.

All pupil equipment is stored in locked units and the IT suite will always be locked after use. Staff computers and laptops will be locked when not supervised by a member of staff.

Using the Internet for learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials. Using the Internet for learning is now a part of the Computing Curriculum (Sept 2014). We teach all of our pupils, at age appropriate stages, how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the computing curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites.
- They are taught how to carry out checks for bias and misinformation

- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

Teaching safe use of the Internet and computing technologies

We will ensure that we promote the 4C's as outlined in Keeping Children Safe in Education 2021. These are:

1. content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
2. contact: being subjected to harmful online interaction with other users; for example: 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'.
3. conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
4. commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The 4Cs will be taught in an age appropriate way as our pupils progress through the school through our computing lessons. Our PDL curriculum and through reminders and specific internet/online safety lessons.

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code (SMART), the thinkuknow website (Think then Click) and Project Evolve to support our teaching in this area: Kidsmart has been developed by the Childnet charity, and is endorsed by the [DfE}, thinkuknow is the CEOP supported website. Project Evolve is a planning resource based on the UK Council for Internet Safety framework statements.

http://www.kidsmart.org.uk

https://www.thinkuknow.co.uk/

https://projectevolve.co.uk/

One of the main aspects of this approach include the following five SMART tips:

- *Safe* - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
- *Meeting* - someone you meet online can be dangerous. Only do so with your parents'/carers' permission and then when they are present...
- *Accepting* - e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...
- *Remember* - someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...
- *Tell* - your parent or carer if someone or something makes you feel uncomfortable or worried...

Suitable material (content)

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Unsuitable material

Despite the best efforts of the filtering systems and school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:

1. Turn off the monitor/screen or close the laptop
2. Making a note of the website URL and any other websites linked to it and time and date it was accessed.
3. Informing the ICT Administrator (Calvin Frampton/Graham Wells)
4. Logging the incident – ICT Incident Log Book in the school office/computer suite
5. Discussion with the pupil about the incident, and how to avoid similar experiences in future

Managing Internet Access

Information system security

The security of the school information systems will be reviewed regularly with virus protection installed and updated regularly. The school uses broadband with effective monitoring and filtering strategies that meet the safeguarding needs of our pupils.

E-mail

Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils 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 an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. (The forwarding of chain letters is not permitted.)

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published – including staff email addresses provided by the school. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully; according to the Multimedia Consent form filled in at the beginning of each academic year, and will not enable individual pupils to be clearly identified. Pupils' full names will not be used anywhere on the Web site or school social media accounts, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or social media accounts – through the Multimedia Consent form. When pupils work is published, on the school's website, social media accounts or newsletter, it will not enable individual pupils to be clearly identified and only shared in a positive light.

Social networking and personal publishing

For more detail see the school's Social media policy.

Social networking sites and newsgroups will be blocked unless a specific use is approved. Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and

clubs etc. Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils and pupils are educated on the age restrictions of these sites.

Managing filtering

The school will work in partnership with the service provider to ensure filtering systems block harmful and inappropriate content without unreasonably impacting teaching and learning. If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school online safety coordinator or the systems administrators. Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. External IP addresses should not be made available to other sites. Under no circumstances should pupils make or answer a videoconference call. Videoconferencing should be supervised appropriately for the pupils' age and always led by a member of staff.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to UK GDPR and the Data Protection Act 2018.

Policy Decisions

Authorising Internet access

The school will maintain a current record of all staff and pupils who are granted Internet access. All staff, including Teaching Assistants and Supply Teachers must read and sign the acceptable ICT Acceptable User Policy (AUP) before using any school computing resource. At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy.

Assessing risks

In common with other media such as magazines, 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, 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.

The Headteacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

Handling Online Safety complaints

Complaints of internet misuse will be referred to a senior member of staff. Any complaint about staff misuse must be referred to the Head teacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (as set out in the Child Protection Policy). A senior member of staff or the class teacher may deal with complaints about pupils internet misuse inside or outside of school. The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Sanctions within the school discipline policy include:

- interview/counselling by class teacher / Headteacher;
- informing parents or carers;
- removal of internet or computer access for a period.

- sanctions in line with our behaviour policy

Communicating the Policy

Introducing the online safety policy to pupils

Rules for Internet access will be posted in all networked rooms. Pupils will be informed that Internet use will be monitored. Advice on online safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

Staff and the Online Safety policy

All staff will be given the School Online Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' / carers' support

Parents' / carers' attention will be drawn to the School Online Safety Policy in newsletters, through Online Safety publications and online safety workshops led by the computing lead.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key Online Safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites. Pupils should be supervised.	Pupils should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick Picsearch safesearch **NOT Google images**
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information.	Consider using systems that provide online moderation e.g. SuperClubs. GridClub School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School website
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	School website
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used.	School Blog Non-internet based models School social media accounts

	Access to other social networking sites should be blocked. Pupils should never give out personal information.	
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	

Appendix 2 Online Safety Audit

This quick audit will help the Senior Leadership Team (SLT) assess whether the basics of online safety are in place to support a range of activities that might include those detailed within Appendix 1.

The school has an Online Safety Policy Y/N

Date of latest update:

The Policy was agreed by governors on:

The Policy is available for staff:

And for parents:

The Designated Child Protection Coordinator is:

The Online Safety Coordinator is:

How is Online Safety training provided?

All staff sign a Computing Acceptable Use Agreement. Y/N

Parents sign and return an agreement that their child will comply with the school Computing Acceptable Use statement. Y/N

Rules for Responsible Use have been set for students: Y/N

These Rules are displayed in all rooms with fixed computers. Y/N

Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access. Y/N

School personal data is collected, stored and used according to the principles of the Data Protection Act.

Y/N

Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT Y/N