ONLINE SAFETY POLICY

Approved by: Cheryl Brake
Last reviewed on: 1st December 2024
Next review due by: 1st December 2025

VICTORIA ROAD PRIMARY SCHOOL

Scope of the Policy

This policy applies to all members of the school (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The school will deal with such incidents within this policy and associated Safeguarding, behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Our Online Safety Policy has been written by the school, building on KCSiE and government guidance. It has been agreed by staff and approved by governors. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online Safety and Safeguarding

Our policy empowers the school to protect and educate our pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorized into four areas of risk:

•content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, radicalization and extremism.

•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'.

•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

•commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

For many adults, there is separation in their minds between 'real life' and the 'online world'. This is a dangerous misconception, as the connected world embraces both online and offline; for young children there is no separation.

Staff have training to ensure that they are aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases this will take place concurrently via online channels as well as in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and prejudicial messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images, to those who don't want to receive such content.

Curriculum

To ensure that the children understand the need to be safe online and what is appropriate to do and say online we have a robust, well-planned and age-appropriate E-safety curriculum. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities, and will be provided in the following ways:

Why the internet and digital communications are important

The Internet is an essential element in the world today and preparing children for life in 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.

Internet use will enhance learning

The school Internet access includes filtering appropriate to the age of our 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 at an age appropriate level in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how 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 how to report unpleasant Internet content to members of staff and this will be dealt with accordingly. Pupil image file names will not refer to the pupil by their full name. Parents are clearly informed of

the school policy on image taking and publishing, both on school and independent electronic repositories.

Managing Internet Access

The School's IT systems security will be reviewed regularly through our LAT IT Management Team and virus protection will be updated regularly. Broadband services provide: - Security Services (Web Hosted): Fortinet FortiGate Firewall and Schools Broadband DDoS Protection
Safeguarding (Web Hosted): Netsweeper Web Filtering: Provides user level web filtering to block harmful and inappropriate online content and where necessary will provide regular reports to the DSL/DDSL's to highlight any attempts to access harmful and inappropriate online content.

New Schools Broadband Safeguarding Incident Management Platform -Provides a real time level of online safeguarding alerts, based on specific key words and access to inappropriate sites (e.g. extremism, pornographic material or drugs) are made within school. If any incidents or exposure to inappropriate content is detected, it will be followed up by the Headteacher/AHT. See Appendix A for record log kept in SCR. The Headteacher/AHT will be informed and they will speak to the person concerned and take the appropriate action, working with the IT department, depending on the nature of the incident.

Teachers have work email accounts to use for the sole use of related emails and these, not personal email accounts, should be used for all school-based communication.

Published content and the school web site

The contact details given on our website are of the school office and key staff.

The Headteacher/AHT and Senior Administrator will take editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

A variety of multimedia, including photographs, videos, and sound clips that include pupils will be selected carefully. Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Written permission will initially be obtained when children start school and yearly thereafter. Parents have the option to request whether or not children's photos are used on our school website and staff are aware of children whose images are not to be shared.

Managing emerging technologies

Emerging technologies will be examined for educational benefit before use in school is allowed. The senior leadership team 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 formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. Mobile phones are allowed to be use in Dedicated spaces by staff and visitors as outlined in the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.

- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose;

- The school's Broadband Internet settings identify staff logins and filters appropriately.

Social Networking and personal publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use. Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

The school works with SWGfL to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher/AHT who will follow the procedure outlined above in Managing Internet access.

Senior staff to ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

Videoconferencing should use the educational broadband network to ensure quality of service and security. Whenever necessary, the use of video conferencing and webcams will be supervised by an adult at all times due to the pupils' age.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. It is made clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.

Handling Online safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a safeguarding nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet.

Policy Decisions

Authorising Internet access

All staff must read and sign the "Staff Code of Conduct and Acceptable Use Policy.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems. At Key Stage 1 and EYFS, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials and within KS2 they will be supervised by an adult whilst within school.

Any person not directly employed by the school must inform the school office and if appropriate will be given the wi-fi password. Supply teachers will be asked to comply with the school's "acceptable use policy" before being allowed to access the internet from the school site.

Reviewing our online safety

Technology, and risks and harms related to it evolve and changes rapidly. We carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks the children face using tools on the 360 safe website.

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

The school uses TME as an IT provider and therefore has a disaster recovery system in place for critical data that includes a secure, remote back up of critical data.

• All computer equipment is installed professionally and meets health and safety standards;

• The school fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable, particularly through the use of Hector Protector.

• The school has a clear, progressive online safety education programme throughout the school.

• All children are to be taught the stay safe 'SMART' rules and to take part in online safety specific activities as part of Safer Internet Day yearly.

Safe: Keep safe by being careful not to give out personal information when you're online

Meet- Meeting someone you have only been in touch with online can be dangerous. Online friends are still strangers even if you have been talking to them for a long time.

Accepting: Accepting emails, messages or files from people you don't know

Reliable: Someone online might lie about who they are and what they might say may not always be true.

Tell: Tell a parent, care or trusted adult if someone, or something, makes you feel uncomfortable or worried, or if you or someone you know is being bullied online

Communications

Introducing the online safety policy to pupils

A programme of training in online safety, based on the Think you know online resources, is being used across Key Stage 1. Online safety training is embedded within the Computing scheme of work.

Staff and the Online Safety policy

All staff will be given the school online safety policy and its importance will be explained. It is also covered in the yearly safeguarding briefing and on-going throughout the year. Staff are informed that network and Internet traffic can be monitored and traced to the individual user. (see above for more detailed training for staff on the safeguarding element of Online safety)

We ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

Top tips for parents and carers

1. Free to Talk

Talk regularly with your child about how they use technology. Find out how they like to represent and express themselves online, and how being online makes them feel. Listening to your child will give you the best possible idea of how you can support them. Not sure where to begin? Have a look at our suggested 'Conversation Starters' for parents and carers.

2. Free to explore differences

The internet is a place where lots of different people can communicate and come together. For some children, the first place they see people who are different to them may be online. For others, the internet may be the one place where they can find people similar to them. Acknowledge the different types of identities your child may see online, and use these to spark discussions around diversity and inclusivity. Talk to your child about being respectful to everyone online, and what to do if they feel their own identity is being targeted.

3. Free to make the internet work for your family

There are lots of tools to help you manage the devices used by your family. For example, knowing how to activate and use parental controls can help protect your child from seeing inappropriate content online. For advice and guidance on how to make use of parental controls and other safety features on devices, check out our free Parents' Guide to Technology.

4. Free to get involved

As parents and carers, it's natural to feel worried about the risks posed by your child being online, but for young people the internet offers a wealth of exciting and fun ways to explore and experiment with their identity. This might be through the characters they choose on games, the filters or emojis they use on profile pictures, the content they share, or the sites and services they use. Spend some time with your child looking at, or interacting with, the things they do online. Talk about both the positive and negative aspects of being online, and empower your child with safe choices they can make - instead of overwhelming them with restrictions.

Appendix A

E-Safety Incident log

ALL e-safety incidents to be recorded by the IT Coordinator. The Head teacher/AHT/ Member of SLT, will monitor this incident log termly. Any incidents involving cyber-bullying may also need to be recorded elsewhere.

Date and Time	**Name of pupil or staff member**	**Computer/device number**	**Details of incident** **(inc. evidence and CPOMS if required)**	**Actions taken**