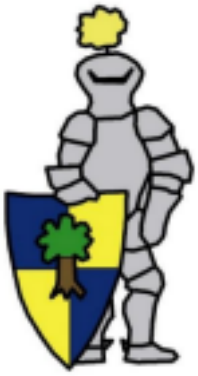
Knightwood Primary School



Online Safety Policy

Name of School:	Knightwood Primary School
Name of Responsible Manager/Headteacher:	Emma Clark – Headteacher
Date Policy approved and adopted:	November 2024
Date Due for review:	November 2026

1. Introduction and principles

Online safety is about helping children to stay safe online. It may also be referred to as internet safety, e-safety or cyber safety. It encompasses the different devices used to access the internet (e.g. PCs, laptops, smartphones, tablets) and different aspects of internet use (e.g. searching online, online chatting, online gaming, electronic sports, email, social media). Being safe online means individuals are protecting themselves and others from online harms and risks.

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

It is important that children become familiar with Information and Communication Technology (ICT) at an early age, to develop the skills they will need for the remainder of their education and in adult life, helping them participate more readily in a rapidly changing world. ICT can help engage, motivate and stimulate children, helping them access new ideas and experiences; it can encourage independent learning and help them develop research and evaluation skills. We use it to support lessons in subjects across the curriculum. We believe that children have the right to enjoy time online and to benefit from the opportunities that this can bring. Our online safety teaching aims to equip children with the knowledge to make the best use of the internet and technology in a safe, considered and respectful way.

We have a **named online safety co-ordinator**,Richard Hebdon. However, a whole-school approach to online safety is essential to protect and educate pupils and staff, and to ensure mechanisms are in place to identify, intervene in, and escalate any concerns where appropriate. It's not the job of one person and it is definitely not just about technical solutions.

This policy is to be considered in conjunction with the Child Protection and Safeguarding Policy, Acceptable Use of ICT Policy, Q1E Data Protection Policy, the school behaviour and anti-bullying policies and the school's computing curriculum. This policy has been written in line with the statutory guidance Keeping Children Safe in Education (DfE, 2024) and Education for a Connected World (UK Council for Internet Safety, 2020).

All staff are required to read this policy.
SAFEGUARDING AND PROMOTING THE WELFARE OF CHILDREN IS EVERYONE'S RESPONSIBILITY.

2. Online safety risks and harms

a. As well as providing many positive opportunities, technology has become a significant component of many safeguarding issues, and can facilitate the exploitation of children. Elements of online activity can also adversely affect wellbeing, in connection with self-image, reputation, health and lifestyle. Any pupil can be vulnerable online, and this can fluctuate depending on their age, developmental stage and personal circumstance.

b. 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 e.g. pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism.
- **Contact:** for example peer to peer pressure, commercial advertising, adults posing as children with the intention to groom or exploit them.
- **Conduct:** online behaviour that causes, or increases the likelihood of, harm; e.g. making, sending and receiving explicit images (such as consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), threatening to reveal images to get someone to do something, online bullying, harmful challenges.
- **CDfE standards for 'Filtering and Monitoring" commerce:** such as online gambling, inappropriate advertising, phishing or scams.

c. Children can also abuse other children online. This can take the form of abusive, harassing and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content.

3. Online filtering and monitoring

a. In school, we ensure children are safeguarded from potentially harmful/inappropriate online material through appropriate internet filtering and monitoring systems following the DfE standards (DfE 2023, Appendix A). We normally block access to social networking sites, but may allow them for specific supervised activities.

b. The capacity and security of our IT systems are reviewed and stress-tested regularly. Virus protection, operating systems and applications are updated regularly. Security strategies are discussed with our IT support provider. New technologies are risk-assessed before use. We also work with our internet service provider to ensure appropriate protections are in place.

c. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the scale and nature of worldwide internet content, it is not possible to guarantee that unsuitable material will never appear on a computer. The school cannot therefore accept liability for material accessed or any consequence of this.

d. The DSL will have lead responsibility for filtering and monitoring

e. All staff will receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring

4. Use of the internet in lessons

a. Internet access in lessons (including when children are asked to undertake online research on their own or in small groups) is managed carefully and appropriately for the age of the pupils, with clear objectives.

5. Mobile phone and email safety

a. We understand some children will bring in mobile phones (or other devices) to school, for example for parent reassurance if they are walking to and from school by themselves. However, they are required to hand in their phones to the teacher at the start of the day. See our Mobile Phone Acceptable Use policy - https://www.knightwood.hants.sch.uk/mobile-phones-and-walking-home-from-school/
b. Occasionally children may make use video conferencing technology as part of a school activity. They may only do this with permission and supervision from a member of staff.
c. Children may only use approved email accounts on the school system.
d. Children must immediately tell a member of staff if they receive an offensive message.

6. Educating children to keep themselves safe

a. Online safety at Knightwood is part of our broad and balanced curriculum and it is delivered across different subjects including computing, PSHE and RSE. We also undertake additional activities for 'Safer Internet Day' each year.
b. Pupils are taught:
    - What internet use is acceptable in school and what is not. Children are informed that their network/internet use will be monitored.
    - That they must not reveal personal details of themselves or others online or in emails, or arrange to meet anyone without specific permission.
    - How to report things that make them feel uncomfortable, unsafe, scared or worried (including reporting inappropriate contact or content through platforms and apps).
    - That their online actions can impact their and others offline lives.
c. **Online safety rules (Appendix B)** are posted in appropriate places in school and the children are reminded of them throughout the year.
d. Pupils also learn (through age-appropriate teaching) about managing online information; self-image and identity; risks of social networking and online gaming including contacting strangers, online bullying and grooming; online relationships; online reputation; privacy and security; copyright and ownership.
e. Some pupils, for example children that are looked after and those with SEND, may be more susceptible to online harm or have less support from family or friends in staying safe online. Support and teaching will be tailored to meet the needs of these pupils.

7. Children's personal data, including names and photographs

a. Parents/carers are asked for their consent for the school/trust to publish photos of their child (e.g. on the website/ in publications). We will not use a child's name beside a photo of them.
b. Children's full names will not be used anywhere on a school website, blog, app or social media page, unless in exceptional circumstances in which parental permission has been obtained (e.g. to celebrate an individual achievement in a news item).
c. We ask parents and carers to support our school community by avoiding posting names, photos or other information about specific pupils or staff online or in message groups.
d. Please refer to our Data Protection Policy for more details on how we manage data.

8. School online content and communications

a. The headteacher will take overall responsibility for the school's website, email or text communications, apps, blogs or social media accounts, and will ensure that all content is accurate and appropriate and suitable protective systems are in place.
b. School communications with parents/carers will proactively promote online safety.
c. Communications from the school's Parent Teacher Association (KSA) (or equivalent) should be in accordance with this policy and the school's Data Protection Policy.

9. Adult awareness of online safety and the acceptable use of ICT

a. All staff are made aware of risk factors (including those summarised in section 2) through whole-school training, including specific Prevent training.
b. All staff, supply staff, local governors and trustees are expected to read and understand the School Code of Conduct, Acceptable Use of ICT Policy and Online Safety Policy.
c. Other visitors and volunteers will be provided with guidance depending on their role
d. Where appropriate, volunteers and visitors will be given limited access to the school network.

10. Helping parents to keep children safe online at home

a. We expect parents and carers to take responsibility for managing their children's responsible use of the internet at home. We will support this by using school communications (including newsletters and school websites) to reinforce the importance of children being safe online, to raise awareness of online safety risks, and to share tips and guidance.
b. If the school asks children to go online for a school-related activity or for homework, we will ensure parents and carers are aware of what this is, which sites they will access and who they will be interacting with online.

11. Remote education

a. Schools will have regard to the government's advice about keeping pupils and staff safe if/when learning remotely (see links in Appendix A).
b. Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor use online. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

12. Handling online safety issues

a. We make sure pupils are able to identify trusted adults in school. Parents and carers should also be made aware of how they can raise concerns with a member of school staff.
b. Issues of internet misuse will be dealt with by a senior member of staff. Any issue or potential issue concerning misuse by a staff member must be referred to the headteacher.
c. Issues concerning child protection must be dealt with in accordance with the Child Protection and Safeguarding policy. Staff are also aware of different ways to access support from school, police, UK Safer Internet Centre and CEOP (see **Appendix A**).
d. Internet browsing history may be looked at in cases where it is deemed necessary.

e. Computers, mobile phones or other devices found to contain images or text relating to a safeguarding concern or inappropriate use may be removed from children in situations where parents or police may need access to the information. Devices may be confiscated without the consent of the child. They should be turned off and kept in a sealed envelope.
f. Inappropriate images will not be printed or saved. They may be deleted with the child's consent or parents may delete images in the presence of the child.
g. Where staff are required to see inappropriate images, messages or other content which has been created/shared/received/stored by a child or member of staff, a written record will be made of when they were seen, who was present and the reason for viewing them.
h. Staff will be offered opportunities for supervision, or managers will ensure time for follow up and reflection following experience of distressing situations.
i. Schools will consider any reports of harmful challenges/online hoaxes, taking into account the scale and nature of possible risk to children, and what support can be given in response.
j. Parents and carers who wish to raise a formal concern should refer to the concerns and complaints policy.

Appendix A: Useful documents, contacts and links

Keeping Children Safe in Education, DfE, September 2024: Statutory safeguarding guidance for schools.
https://assets.publishing.service.gov.uk/media/6650a1967b792ffff71a83e8/Keeping_children_safe_in_education_2024.pdf

Safer Internet online Safety Helpline: 03443814772; helpline@saferinternet.org.uk; www.saferinternetknow.org

UK Safer Internet Centre: report harmful online content: https://reportharmfulcontent.com/

Child Exploitation and Online Protection (CEOP): A law enforcement agency which aims to help keep children safe from sexual abuse and grooming online. Anyone can report directly to CEOP if something has happened online which has made them feel unsafe, scared or worried. https://ceop.police.uk/
CEOP also provide advice (for anyone) on staying safe online, at www.thinkuknow.co.uk/.

UK Council for Child Internet Safety (UKCCIS): A group of over 200 organisations that work in partnership to help keep children safe online. They produce a wide range of reviews and guidance for schools and parents.
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

NSPCC e-safety resources: Online safety advice and resources for schools
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/e-safety-schools/

Keeping safe online: Guide for people with learning disabilities (Care Management/ CHANGE)
http://cmg.co.uk/wp-content/uploads/2017/12/Keeping-Safe-Online-Easy-Read-Guide-EmailVersion.pdf

Searching, screening and confiscation, January 2018
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf

Online Harms White Paper https://www.gov.uk/government/consultations/online-harms-white-paper

Teaching Online Safety in School, Jan 2019
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

Education for a Connected World, updated 2020: A framework to equip children for digital life.
https://www.gov.uk/government/publications/education-for-a-connected-world

Vulnerable children in a digital world
www.internetmatters.org/about-us/vulnerable-children-in-a-digital-world-report/

Harmful Challenges and Online hoaxes, Feb 2021
https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes

Remote Education guidance relating to safeguarding:
DfE guidance: https://www.gov.uk/guidance/safeguarding-and-remote-education
NSPCC advice: https://learning.nspcc.org.uk/news/covid/undertaking-remote-teaching-safely

Filtering and Monitoring Standards , Feb 2023:
https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges
Additional guidance on filtering and monitoring can be found at: UK Safer Internet Centre: "appropriate" filtering and monitoring.
https://www.saferinternet.org.uk/advicecentre/teachers-and-school-staff/appropriate-filtering-and-monitoring .

Appendix B: Online safety posters for children

Key Stage One:

Key Stage Two:

Stay safe online

Quality First
Education Trust