Online Safety Policy

The Cottesloe School

Policy Type:	Non - Statutory
Reviewed by:	Mrs C Hankin (Assistant Headteacher), Mr S Clawson (Head of Year 10 and Strategic Digital Lead) and Mrs C Stirk (Policies Governor)
Date:	Spring Term 2026
Approved by:	Strategy Committee - Jan 2026
Last reviewed:	Autumn Term 2018
Next review:	Autumn Term 2026

Contents

Online safety encompasses internet technologies and electronic communications such as mobile phones, wireless technology, and AI-generated messages and content. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The School's Online Safety Policy will operate in conjunction with other policies including those for:

- Behaviour for learning and use of reasonable force
- Anti-Bullying
- Safeguarding
- Digital Technology Acceptable Use
- Privacy Notice (for both staff and students)

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of the Online Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband service including the effective management of web filtering.

June 2025

The Cottesloe School Online Safety Policy – Spring Term 2026

1. Implementing and reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for Digital Technology/ICT, Anti-bullying, and Safeguarding. This policy is an integral part of the school's overall safeguarding framework, adopting a whole-school approach to online safety.

The Cottesloe School has an Online Safety Coordinator who is the Designated Safeguarding Lead, as the roles overlap. Clear roles and responsibilities for online safety management are established for all staff and governors, with a member of the Senior Leadership Team and a governor specifically responsible for ensuring online safety standards are met.

Our Online Safety Policy has been written by the School, building on Bucks Council Online Safety Policy and government guidance. It has been agreed by the Senior Leadership Team (SLT) and approved by Governors.

The Online Safety Policy and its implementation will be reviewed annually or earlier if any legislative changes or emerging risks necessitate an update.

The Online Safety Policy was revised by Simon Clawson (Digital Lead) and Chloe Hankin (Designated Safeguarding Lead).

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones, tablets and smart watches;
- Internet communications: e-mail, direct messaging & other instant messaging methods;
- Webcams and videoconferencing;
- Wireless or wired games consoles.
- AI generated messages and content.

What are the risks?

- Receiving inappropriate content;
- Predation and grooming (including for radicalisation, drug trafficking, and financial gain);
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats (including cyberbullying affecting students and staff) ;
- Identity theft;
- Publishing inappropriate content;
- Online gambling and in-app/game purchasing ;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches (including phishing and ransomware) ;
- Corruption or misuse of data;
- Exposure to AI-generated content and deepfakes (manipulated or fabricated visuals/sounds) ;
- Misinformation and disinformation (false or misleading information) ;
- Risks associated with online gaming platforms (e.g., inappropriate content, unknown contacts, overuse) ;
- Exposure to online misogyny and other problematic ideas from influencers.

If there is a suggestion that a student is at risk of abuse or significant harm, the matter will be dealt with under the school's safeguarding procedures.

2. Teaching and learning

2.1 Why internet use is important

The purpose of internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's Management information and administration systems. Internet use is part of the National Curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction.

Access to the internet is an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality internet access. Students will use the internet both in and outside of school and will need to learn how to evaluate internet information and to take care of their own safety and security.

2.2 How internet use benefits education

Benefits of using the internet in education include, but not limited to:

- access to learning wherever and whenever convenient;
- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between students world-wide;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational; materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Bucks Council and Department for Education;
- access to learning wherever and whenever convenient.

2.3 Internet use will enhance learning

The School internet access will be designed expressly for student use and will include filtering appropriate to the age of students. Filtering includes use of firewalls and monitoring software to block/restrict access to sites based on keywords and content types. This system will be balanced to avoid excessively restricting the day-to-day educational needs of the school or preventing students from learning how to recognise risk themselves.

Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Constant monitoring will be used to reinforce what is and is not acceptable.
Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.

Any sites that staff or students feel would be useful to access will be reviewed and whitelisted if deemed appropriate or of value to the curriculum.

Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.4 Students will be taught how to evaluate internet content

The school should ensure that the use of internet derived materials by staff and by students complies with copyright law.

Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy, e.g., 'fake news', and to identify misinformation and disinformation. They will learn to recognise techniques used for persuasion, such as persuasive design and online fraud.

Students will be taught:

- To acknowledge the source of information used and to respect copyright when using internet material in their own work.
- About the risks associated with using the internet and how to protect themselves and their peers from potential risks, including the dangers of AI-generated content and deepfakes.
- How to recognise suspicious, bullying or extremist behaviour, and understand the influence of online misogyny and other problematic ideas from influencers.
- The definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.
- The consequences of negative online behaviour.
- How to report cyberbullying and/or incidents that make students feel uncomfortable or under threat, and how the school will deal with those who behave badly, using clear, child-friendly reporting mechanisms.

3. Managing Information Systems

3.1 Information system security

The security of the school information systems will be reviewed regularly.
Robust antivirus software will be updated regularly. Security strategies will be compliant with local and national guidelines and will be reviewed regularly. Personal data sent over the internet will be encrypted or otherwise secured. The school will use an encrypted and password-protected WiFi network. Portable media may not be used without specific permission followed by a virus check. Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mails. Files held on the schools network will be regularly checked. The Network Manager will review system capacity regularly.
Memory sticks should not be used on the school network without express permission, and only for the necessary transfer of work to external bodies such as exam boards. All memory sticks should be scanned for viruses and encrypted with a suitable method.
Consideration will be given to advanced security measures such as regular, independent penetration testing and strategic investment in threat intelligence to proactively identify and address vulnerabilities. Protocols will be in place to address internal risks, including unauthorised accessing of files or networks by students or staff.

3.2 E-mail

The school uses email internally for staff and students and externally for contacting parents and conducting day to day school business and is an essential part of school communication. The school has the right to monitor emails, attachments and their contents but will only do so

if there is suspicion of inappropriate use. Staff and students should regularly change passwords and ensure that passwords are effective.

Students should be aware of the following when using email in school:

- Students will be taught to follow these guidelines through the IT curriculum and in any instance where email is being used within the curriculum or in class.
- All students are provided with a school gmail account and students may only use approved email accounts on the school system during school hours.
- Students should not use their personal email accounts to contact staff. Staff should not respond to any further emails from the original email account unless the nature of the communication raises safeguarding concerns.
- Students are warned, via the Acceptable Use Agreement not to reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Students should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Access in school to external personal e-mail accounts will be blocked.
- E-mail sent to an external organisation should be written carefully.
- The forwarding of chain letters, 'jokes' or offensive material is not permitted.

Staff should be aware of the following when using email in school:

- Staff should use their school email accounts for school-related matters, contact with other professionals for work purposes and to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people.
- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by a member of the Leadership Team.
- Staff must tell a member of the Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Staff should refer to the Data Protection and Confidentiality Policies before sending any sensitive or personal data via email.
- E-mail sent to an external organisation should be written carefully and staff should adhere to guidance in the staff code of conduct.
- The forwarding of chain letters, 'jokes' or offensive material is not permitted.

3.3 Published content and the School website

The school website is viewed as a useful tool for communicating the school ethos and practice to the wider community. It is also a valuable resource for prospective parents and students, current parents, students and staff for keeping up-to-date with school news and events, celebrating whole-school achievements, personal achievements and promoting the school. The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered, by the Leadership Team, in terms of safety for the school community, copyrights and transparency policies. The website

will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

- The contact details on the website should be the School address, e-mail and telephone number. Staff or students personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material will be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- Annual audits of online content will be conducted to ensure appropriate use of images and videos.
- A 'Names-No-Images / Images-No-Names' policy will be implemented for student photographs to reduce identification risks.
- Public access to sensitive content will be restricted using password-protected platforms where appropriate.
- Metadata will be removed from images, lower resolution files used, and strict privacy settings applied on social media accounts to further protect students from potential misuse.

3.4 Publishing students' images and work

Photographs that include students will be selected carefully and any student whose photos are used will need to have parents' permission for these to be published.
Students' full names will not be used anywhere on the website or on social media, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of students or their work are published on the School Website.
Work can only be published with the permission of the student and parents.
The principles outlined in section 3.3 regarding secure management of images and videos will be applied to all published student images and work.

3.5 Social networking and personal publishing

The school encourages parents with children under the age of 13 to follow the guidance of social media sites such as Facebook, Snapchat etc. and not give their child access.

The Cottesloe School will block/filter access to social networking sites, except for the purpose of the school social media accounts used by selected staff members.
Students will be 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 attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
Students should be advised not to place personal photos on any social network space. They

should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or School.
Teachers should be advised not to run social network spaces for student use on a personal basis.
Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are always representing the school and must act appropriately.
The Cottesloe School is aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments.
Staff that have any social networking sites shouldn't have any links connecting them to The Cottesloe School visible on their page(s).
School maintained social media accounts will be monitored on a regular basis and can be viewed through the school website.
Staff are strongly advised not to have any social networking accounts; however, those that choose to have one must ensure that their security settings are set to the highest available.

3.6 Managing Monitoring and Filtering

The Cottesloe School will work in partnership with external agencies to ensure systems to protect students are reviewed regularly, in line with Department for Education (DfE) guidance and the UK Safer Internet Centre's (UKSIC) 2025 Appropriate Filtering and Monitoring Definitions.
If staff or students discover an unsuitable site, it must be reported to the Online Safety Coordinator and the Network Manager.
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
Any material that the School believes to be illegal must be reported to appropriate agencies such as CEOP (Child Exploitation & Online Protection Centre).
The Cottesloe School uses Talk Straight to filter the school users' access to the internet.
The school uses Smoothwall Monitor to monitor school accounts for both staff and student accounts. This is both inside and outside of school where individuals use their school accounts on school purchased devices only.
Any inappropriate or concerning use is flagged to members of the school safeguarding team where appropriate action is taken. Monitoring will also address internal risks, such as unauthorised access by students or staff.
This could include, but not limited to:

- A learning conversion
- Parental/ carer contact
- Disciplinary action in line with the schools behaviour for learning and use of reasonable force policy
- External agency referrals

3.6.1 Contact with violent extremists

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances some young people may be susceptible to these influences. Bucks LA provides interventions under the Channel project which is part of the Government's Prevent Strategy to divert young people away from extremism.

Staff need to be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups. The school will ensure that adequate filtering is in place, with a review of filtering taking place whenever there is any incident of a young person accessing websites advocating violent extremism.

The Online Safety Co-ordinator, along with the Network Manager, should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting young people. If there is evidence that a young person is becoming deeply enmeshed in the extremist narrative, staff will seek advice from Bucks Prevent Officer external agencies to prevent radicalisation.

3.7 Managing videoconferencing and audio conferencing

The equipment and network

The school uses school-owned laptops and chromebooks for all video and audio conferencing.
Google Meet is the preferred method for all in school meetings, with Teams, Zoom and School Cloud being used where needed.
All videoconferencing equipment in the classroom must be switched off when not in use.
The equipment must be secure and if necessary locked away when not in use.
External IP addresses should not be made available to other sites.
Videoconferencing contact information should not be put on the School Website.

Users

Students should ask permission from the supervising teacher before making or answering a videoconference call.
Videoconferencing should be supervised appropriately for the students' age.
Parental permission will be sought for children to take part in videoconferences, this includes photographic permissions.
Only key administrators should be given access to the videoconferencing system, web or other remote control page.
Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
Recorded material shall be stored securely.
If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
Videoconferencing is a challenging activity with a wide range of learning benefits.
Preparation and evaluation are essential to the whole activity.
Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that the material being delivered is appropriate for the students.

For any external speakers, a visitor external speaker checklist form should be completed. This can be found on the TCS Hub.

3.8 Managing mobile and emerging technologies

Mobile phones and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- They can make students and staff more vulnerable to cyberbullying
- They can be used to access inappropriate internet material
- They can be a distraction in the classroom
- They are valuable items that could be stolen, damaged or lost
- They can have integrated cameras, which can lead to safeguarding, bullying and data protection issues due to the nature of technology and its rapid changes. This policy can be subject to review and update when a significant new development is identified.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to all members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. This includes derogatory comments posted about staff by parents and children on social media. Any incidents of cyberbullying will be dealt with in accordance with the behaviour for learning and use of reasonable force policy and, where appropriate, the school's Safeguarding Policy. The school's approach will be presented via a whole-school policy, regularly reviewed, communicated to all stakeholders, and linked to other relevant

documents like behaviour, IT acceptable usage, safeguarding, and mobile phone policies.

Emerging Technologies (including AI)

The school has a published AI policy which all staff are required to follow.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. For AI tools, risk assessments will specifically consider data privacy implications, with strict guidelines prohibiting the input of sensitive personal, student, or internal school data into public AI models.

Online Gaming Platforms

Online gaming is acknowledged as a pervasive activity for students, offering potential benefits such as fostering teamwork and improving social skills. However, the policy will address associated risks including cyberbullying, exposure to inappropriate or harmful content (e.g., sexualised or violent material), grooming, in-app/game purchasing and gambling, overuse of screens leading to 'addiction', and receiving requests or messages from unknown people. Education will focus on responsible engagement, age-appropriate game selection, and the effective application of parental controls, rather than outright prohibition.

Mobile Phones

Mobile phones will not be used and must be switched off whilst in school until 3pm.
The sending of abusive or inappropriate text messages is forbidden as is the videoing or photographing of others without permission.
Staff will be issued with a school phone where contact with students is required, for example on school trips.
Wireless network connection is available for both staff and sixth form student owned mobile devices. This is also applicable to laptops owed by staff, sixth form and students that have purchased their own chromebooks outside of the school portal.. Access is only available via the Network Manager once a virus check has taken place. Once accessed the user is still bound by the access restrictions as per the school network.
Students will need to remove any smart watches along with mobile phones whilst sitting any exams, these will be kept in students bags outside of the exam room.
Staff are not permitted to use their mobile phones whilst in school, with the exception of in the staff room, staff work room or personal offices. However, this is only applicable when there are NO students present.
Staff are encouraged to not access their school emails on their mobile devices.

3.9 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the UK General Data Protection regulation(UKGDPR)The school will identify what personal data is collected and why, ensure data is stored securely with proper access controls, appoint a Data Protection Officer (DPO) to oversee compliance, and implement clear policies for data handling and breach management. The school will register annually with the Information Commissioner's Office (ICO) as a Data Controller. A Data Breach Response Plan will be in place to enable swift and compliant action in the event of a data security incident. Data breach response plan

All data processing activities will be conducted in line with The Cottesloe School GDPR policy, which details how data is collected, stored and used in online and offline environments. The school will adhere to the ICO Children's Code (Age Appropriate Design Code), ensuring that children's profiles are private by default, geolocation settings are turned off by default, profiling for targeted advertisements is off by default unless compelling justification exists, We use Public Task and legitimate interests as our lawful basis for processing data.

All staff will receive regular training on data protection practices, including the privacy implications of using AI tools.

4. Policy Decisions

4.1 Authorising Internet access

The internet is used in school by staff and students on a daily basis and as a member of the school community, it is a given that all will use the internet.

4.2 Assessing risks

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and linked nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a School computer. Neither the School nor Bucks ~~County~~ Council can accept liability for the material accessed, or any consequences resulting from internet use.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
Methods to identify, assess and minimise risks will be reviewed regularly. This includes regular, independent penetration testing and strategic investment in threat intelligence to proactively identify and address vulnerabilities.
The Headteacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.
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.
Monitoring and filtering software is in place to prevent misuse.
Methods to identify, assess and minimise risks will be reviewed regularly.

4.3 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; if it is against the Headteacher then the Chair of Governors must be informed.
Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.
Students and parents will be informed of the complaints procedure which can be found in the Complaints and Resolutions Procedure via the school website. Pupils will be explicitly clear about the school's child-friendly reporting mechanisms.1
Parents and students will need to work in partnership with staff to resolve issues.
As with drug related issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
Sanctions within the Behaviour for learning and use of reasonable force Policy include, but are not restricted to:

- interview/talking with the Head of Year;
- informing parents or carers;
- removal of internet or computer access for a period of time. These sanctions will be applied consistently to all members of the school community (students, parents, staff) where appropriate. Students and staff will be made aware of and have easy access to internal and external support avenues, including the National Crime Agency's Click CEOP reporting service, Childline, the Internet Watch Foundation, the Professionals Online Safety Helpline, and GamCare's Young People Service for gambling-related harms.

Harmful Online Challenges and Hoaxes

The school will adopt a measured, evidence-based protocol for responding to harmful online challenges and hoaxes. This will include a case-by-case assessment of risk, verification of facts with reliable sources (e.g. Professionals Online Safety Helpline), and a procedure against publicly naming hoaxes to avoid inadvertently increasing exposure to distressing content. The focus will be on reinforcing general online safety principles, critical thinking, and clear reporting pathways, rather than amplifying the challenge or hoax itself.

4.4 Community use of the Internet

The School will liaise with local organisations to establish a common approach to Online Safety.
The School will be sensitive to internet related issues experienced by students outside of School, e.g. social networking sites. Advice and guidance will be provided to support students, parents and carers with reporting and following up on these.
A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home internet use, co-designing programmes to reflect emerging issues they are hearing about or facing online, or implementing peer-to-peer support schemes. Consistent messaging and shared understanding between school and home will be fostered.

5. Communication of the Policy

5.1 Introducing the Online Safety Policy to Students

Students will be informed that network and internet use will be monitored.
Online Safety will be included in the curriculum to raise the awareness and importance of safe and responsible internet use. This will equip pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, including critical evaluation of online content.
Instruction in responsible and safe use should precede internet access.
An Online Safety module will be included in the PSHCE and ICT programmes covering both school and home use.

5.2 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.
Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
Staff training in safe and responsible internet use and on the School Online Safety Policy will be provided as required. This ongoing training will cover new technologies, evolving risks (e.g., AI privacy implications, online misogyny), legal duties, and effective incident response.
All staff are required to complete a cyber security and safety training session annually from NCCS

5.3 Enlisting parents' support

Parents' attention will be drawn to the school Online Safety Policy in newsletters and on the school Website.
Internet issues will be handled sensitively, and parents will be advised accordingly.
A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home internet use, and guidance on managing online gaming risks.
Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
Parents will need to also sign an Online Safety Acceptable Use Agreement.

6. Online safety Contacts and References

- Childline: http://www.childline.org.uk/
- Child Exploitation & Online Protection Centre (CEOP): http://www.ceop.gov.uk
- Grid Club and the Cyber Cafe: http://www.gridclub.com
- Internet Watch Foundation: http://www.iwf.org.uk/
- Kidsmart: http://www.kidsmart.org.uk/

- Think U Know website: http://www.thinkuknow.co.uk/
- Professionals Online Safety Helpline: 0344 381 4772 / helpline@saferinternet.org.uk
- GamCare Young People Service (for gambling harm): https://www.gamcare.org.uk/get-support/talk-to-us-now/
- National Cyber Security Centre (NCSC): https://www.ncsc.gov.uk/
- Report Harmful Content: https://reportharmfulcontent.com/

7. Review

This policy will be reviewed every year (earlier if any legislative change or emerging risk is identified).

Spring Term 2026

Chromebook Loan Agreement

https://docs.google.com/document/d/12QN_UBOHOEeN4GCmehBwmg46pvxmgg_y/edit

Works cited

1. Teaching online safety in schools - GOV.UK, https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools
2. Online safety policy - UK Safer Internet Centre, https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/online-safety-policy
3. Online safety and schools - NSPCC Learning, https://learning.nspcc.org.uk/online-safety/online-safety-for-schools
4. Online Grooming advice and risks | Internet Matters, https://www.internetmatters.org/issues/online-grooming/
5. How teachers, parents and carers can spot and prevent online grooming and radicalisation, https://www.britishcouncil.org/voices-magazine/how-spot-and-prevent-online-grooming-and-radicalisation
6. Cyberbullying in schools | National Education Union, https://neu.org.uk/advice/health-and-safety/harassment-bullying-and-violence/cyberbullying-schools
7. Cyber security breaches survey 2025: education institutions findings - GOV.UK, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings
8. Preventing misinformation and disinformation in online filter bubbles, https://commonslibrary.parliament.uk/research-briefings/cdp-2024-0003/
9. Responding to the AI deepfake threat: A call to action for school leaders - Sec Ed, https://www.sec-ed.co.uk/content/best-practice/responding-ai-deepfake-threat-school-leaders/
10. Press Notice: Children's Commissioner calls for immediate ban of AI apps that enable 'deepfake' sexual abuse of children, https://www.childrenscommissioner.gov.uk/news-and-blogs/press-notice-childrens-commissioner-calls-for-immediate-ban-of-ai-apps-that-enable-deepfake-sexual-abuse-of-children/
11. Summer riots 'show consequences of dangerous fake news' | University of Leeds,

https://www.leeds.ac.uk/news-business-economy/news/article/5641/summer-riots-show-consequences-of-dangerous-fake-news
12. Gaming In Education The Rise And Benefits | Coconnect, https://coconnect.co.uk/gaming-in-education/
13. Harmful online challenges and online hoaxes - GOV.UK, https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes
14. Tackling Harmful Online Content for Our Children - Timeout Homes, https://www.timeouthomes.co.uk/post/tackling-harmful-online-content-for-our-children
15. New Guidance: Best Practices for Managing Images and Videos on School Websites, https://saferinternet.org.uk/blog/new-guidance-best-practices-for-managing-images-and-videos-on-school-websites
16. UK Safer Internet Centre: Homepage, https://saferinternet.org.uk/
17. What is GDPR and Why Does It Matter In Schools? - Computeam, https://www.computeam.co.uk/videos-and-blog/article/what-is-gdpr-and-why-does-it-matter-in-schools
18. GDPR Compliance for Schools | Education Authority Northern Ireland, https://www.eani.org.uk/schools/policies-and-guidance/data-protection-guidance/gdpr-compliance-for-schools
19. Protecting children's privacy online: Our Children's code strategy | ICO, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/
20. UK Safer Internet Centre - Resources - Educate Against Hate, https://www.educateagainsthate.com/resources/uk-safer-internet-centre/
21. Inappropriate or explicit content - NSPCC, https://www.nspcc.org.uk/keeping-children-safe/online-safety/inappropriate-explicit-content/
22. Online Challenges - UK Safer Internet Centre, https://saferinternet.org.uk/online-issue/online-challenges
23. Cyber Security - GCHQ.GOV.UK, https://www.gchq.gov.uk/section/mission/cyber-security