Online Safety Policy

Agreed by the Governing Body in:	September 2026
Review Date:	September 2027
Review Schedule:	Annually
Person(s) Responsible:	Michael Smith

Online Safety Policy

Our Aims

As a school, we aim to:

- Have **robust and regularly reviewed** processes in place to ensure the online safety of pupils, staff, volunteers, and governors.
- Deliver an **effective, up-to-date** approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish **clear and swift** mechanisms to identify, intervene, and escalate an incident, where appropriate.
- Be consistently proactive to threats, opportunities and risks presented by being online in school.

Application of this Policy

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents, carers, visitors, and community users) who have access to and use school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where permitted), use of school devices by staff offsite and during school-led activities off-site. This policy also applies to staff, pupils, visitors, volunteers, governors and contractors accessing school systems.

The Four Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as grooming, online harassment, cyberstalking, and coercion.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., sharing nudes or deepfake content), cyberbullying, and engaging in harmful online trends or challenges.
- **Commerce** – risks such as fraud, financial scams, fake investment schemes, gambling, and exposure to predatory marketing tactics.

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education (2026 update), and its advice for schools on:

- Teaching online safety in schools.
- Preventing and tackling bullying, including cyber-bullying and digital safeguarding.
- Dealing with image-based abuse (e.g., sharing explicit images).
- Relationships and sex education.
- Searching, screening, and confiscation (updated guidance for handling mobile devices and social media misuse in schools).
- Government guidance on AI safety in education and digital ethics.

This policy also takes into account The Online Safety Act 2023, The Children's Code (UK GDPR for digital services), and the National Curriculum computing programmes of study.

Roles and Responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will review online safety reports termly, co-ordinate regular meetings with appropriate staff, and monitor online safety logs as provided by the designated safeguarding lead (DSL) and ICT Coordinator and Online Safety Lead.

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy and that it is implemented consistently across the school.

The headteacher will ensure that all staff receive annual online safety training, with regular updates throughout the year to reflect emerging risks and changes in statutory guidance.

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead (DSL) and Online Safety Lead.

The headteacher and Online Safety Lead will receive weekly automated reports from AI-powered SmoothWall monitoring.

The Designated Safeguarding Lead (DSL)

The DSL (Mrs. Price) and deputies (Ms. Bogart and Mr. Spinola) take lead responsibility for online safety, in particular:

- Supporting the Senior Leadership team and ICT Coordinator and Online Safety Lead to ensure staff understand this policy and its consistent application.
- Ensuring all staff receive annual online safety training and regular updates throughout the year.
- Monitoring and responding to AI-generated risks, such as deepfake content or AI-assisted cyberbullying.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Liaising with other agencies and/or external services if necessary.

The ICT Coordinator and Online Safety Lead & Online Safety Lead

The ICT Coordinator and Online Safety Lead (Michael Smith) are responsible for:

- Implementing filtering and monitoring systems to block inappropriate content.
- Reviewing all breaches of filter policies and acting where necessary.
- Ensuring that the school's ICT systems are secure against phishing, malware, and AI-driven cyber threats.
- Maintaining, monitoring and reporting on the SmoothWall software, which will aid in filtering and monitoring.
- Communication to the ICT Coordinator and Online Safety Lead from Smoothwall will consist of:

- Low level alerts are stored in the Dashboard for viewing at the next login.
- Medium alerts are communicated through email.
- High alerts are conveyed by phone.

For further information about how we monitor activity and filter safe online usage, please refer to our Filtering and Monitoring Policy on the school website.

Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully, and responsibly.
- Recognize acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.
- Understand AI-generated misinformation, deepfake risks, and digital ethics.
- Understand that many social media platforms have minimum age requirements and the importance of following platform age restrictions.

Teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse, and pupils with SEND.

Cyber-bullying and Digital Misuse

To help prevent cyber-bullying, the school will:

- Educate pupils about the risks of AI-generated abuse, deepfake images, and anonymous harassment.
- Encourage pupils to report any incidents of cyber-bullying.
- Monitor and flag harmful content in real-time.

Pupils Using Mobile Devices, smart watches and recording devices in School

- Pupils may bring mobile devices and smart watches into school. Mobile phones and smartwatches are handed in at the start of the school day and returned at 3.30pm.
- Smart devices that are primarily designed for recording such as 'Meta glasses' are strictly forbidden.
- Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy.

How Will the School Respond to Misuse?

Where a pupil misuses the school's ICT systems or internet, immediate action will be taken, including:

- Restricting digital access.
- Involving parents in online safety discussions.
- Referral to external safeguarding agencies, if necessary.

Use of Artificial Intelligence (AI)

Staff must use AI tools responsibly and in accordance with the school's Acceptable Use Policy. Staff must not enter confidential, safeguarding or identifiable pupil information into unapproved AI systems. Any AI-generated content used for school purposes must be checked for accuracy, appropriateness and potential bias before use.

Appendix 1

EYFS and KS1 acceptable use agreement (pupils and parents / carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: SUGGESTIONS FOR PUPILS AND PARENTS/CARERS

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

Appendix 2

KS2 acceptable use agreement (pupils and parents / carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: SUGGESTIONS FOR PUPILS AND PARENTS/CARERS
Name of pupil:
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • If I bring a personal mobile phone, smartwatch or other personal electronic device into school, I will hand it in at the start of the school day in accordance with the school's procedures and not access it again until it is returned at the end of the school day. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**