Online Safety Policy

Meanwood CE Primary School

Approved by:	Board of Governors	**Date:** 01.09.26
Last reviewed on:	01.09.26	
Next review due by:	01.09.27	

Vision and Values

Open Hearts | Open Minds | Open Arms
Our vision is to enrich the lives of our children emotionally, physically, spiritually and academically, where every person is valued, nurtured and empowered. Our vision is underpinned by Jesus' commandment to "love one another as I have loved you" (John 15:12).

At Meanwood C of E Primary School we will continuously strive to ensure that everyone in our school is treated with respect and dignity. Each person in our school will be given fair and equal opportunities to develop their full potential with positive regard to gender, ethnicity, cultural and religious background, faith, sexuality or disability. The school will provide an inclusive curriculum, which will meet the needs of all its pupils including those with disabilities, special educational needs, from all cultural backgrounds and faiths and pupils with English as an additional language.

1. Aims and Core Principles

Meanwood C of E Primary School aims to establish robust, comprehensive processes to ensure the online safety of pupils, staff, volunteers, and governors. We aim to deliver an effective approach to online safety that empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones'). Crucially, the school is committed to establishing clear, rapid mechanisms to identify, intervene in, and escalate online safety incidents where appropriate.

1.1 The Four Key Categories of Risk (The '4 Cs')

To protect children effectively, the school's online safety strategy is structured around the DfE's four key categories of risk:

Content: Being exposed to illegal, inappropriate or harmful content. This includes pornography, misinformation, disinformation, fake news, conspiracy theories, online misogyny, racism, self-harm, suicide, antisemitism, radicalisation, and extremism.

Contact: Being subjected to harmful online interaction with other users. This includes peer-to-peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom, radicalise, or exploit them for sexual, criminal, financial, or other purposes.

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm. This includes making, sending, and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes or youth-produced sexual imagery), online bullying, harassment, and the spreading of malicious comments.

Commerce: Risks associated with commercial exploitation and financial scams. This includes online gambling, inappropriate advertising, phishing, identity theft, financial fraud, and unauthorized or hidden in-app purchases.

2. Legislation and statutory guidance

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

- Teaching Online Safety in Schools (DfE)
- Mobile Phones in Schools (DfE Statutory Guidance, June 2026)
- Preventing and Tackling Bullying and Cyber-bullying: Advice for Headteachers and School Staff
- Relationships Education, Relationships and Sex Education (RSE) and Health Education (and the statutory RSHE Hub updates)
- Searching, Screening and Confiscation: Advice for Schools (DfE)
- Protecting Children from Radicalisation: The Prevent Duty

It also reflects existing legislation, including but not limited to the Education Act 1996, the Education and Inspections Act 2006, the Equality Act 2010, the Education Act 2011, and the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Board

The Governing Board has overall statutory responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Governing Board must ensure that online safety is an interrelated and running theme within the school's broader safeguarding approach. All governors must read and understand this policy, adhere to acceptable use terms, and ensure that online safety education is personalized and adapted for vulnerable pupils, victims of abuse, and pupils with Special Educational Needs and Disabilities (SEND).

3.2 The Headteacher

The Headteacher is responsible for ensuring that all staff members understand this policy and that it is implemented consistently across the school. The Headteacher has overall operational responsibility for establishing secure online safety procedures.

3.3 The Designated Safeguarding Lead (DSL) Ella Parker

The DSL, Ella Parker, takes lead responsibility for the safeguarding elements of online safety. Her duties include:

- Managing all online safety safeguarding issues and logging incidents in the central Safeguarding File.
- Supporting the Headteacher in ensuring staff understand the policy and that it is applied consistently.
- Working with the external IT provider (Next Generation) to review weekly filtering and monitoring reports, address security incidents, and follow up on alerts.

- Ensuring incidents of cyber-bullying are logged and dealt with in accordance with the Behaviour Policy.
- Updating and delivering staff training on online safety, and providing regular safeguarding reports to the Headteacher and Governing Board.

3.4 The Tripartite IT Governance Structure (Next Generation & School Leadership)

To ensure that online safety is never treated solely as an IT issue or a safeguarding issue in isolation, Meanwood operates a tripartite collaborative structure consisting of the Headteacher (ICT Manager), the DSL (Ella Parker), and the school's external IT service provider (Next Generation).

The IT service provider, Next Generation, is responsible for:

- Implementing, maintaining, and updating appropriate technical filtering and monitoring systems.
- Ensuring the school's ICT systems are secure, protected against malware, and automatically patched.
- Conducting a full security check and monitoring the school's systems on a weekly basis.
- Blocking access to dangerous, inappropriate, or illegal sites and preventing dangerous downloads.
- Using the DfE's 'Plan Technology for Your School' self-assessment tool in collaboration with the Headteacher and DSL to evaluate and upgrade filtering and monitoring systems annually.

4. Educating pupils about online safety

Online safety is integrated into the National Curriculum for computing, PSHE, and the statutory relationships and health education curriculum. Teaching is tailored to be age-appropriate and is adapted for pupils with SEND or other vulnerabilities.

By the end of primary school, pupils will know and understand:

- Online Relationships: That the same principles of respect, boundaries, and kindness apply to online relationships as face-to-face, including when anonymous.
- Critical Digital Literacy: How to critically analyze online information, recognize risks, fake news, misinformation, and the risks associated with people they only know online.
- Advanced Harms: Age-appropriate awareness of emerging harms, including generative AI risks, deepfakes, online misogyny, incel culture, and online harassment.
- Data & Privacy: How personal data is shared, tracked, and used online, and how to keep personal details private.
- Reporting Concerns: How to recognize unacceptable online behaviour, and identify multiple distinct paths to report content or contact concerns.

5. Educating parents about online safety

The school actively works with parents to promote a consistent online safety culture. We raise awareness through letters, newsletters, the school website, our Facebook account, and Arbor communications. Parents are informed of the filtering and monitoring systems used in school, and the safe digital spaces their children access for learning. Parents are expected to support the school's acceptable use agreements and report any online safety concerns to the Headteacher or DSL.

6. Cyber-bullying

Cyber-bullying is defined as repetitive, intentional harm conducted online (through social media, messaging apps, or gaming). It is strictly prohibited. The school actively prevents cyber-bullying through PSHE lessons and classroom discussions. Incidents are dealt with in accordance with the Behaviour Policy. Where harmful or inappropriate material is spread among pupils, the school will act immediately to contain it. If there are reasonable grounds to suspect a criminal offense, the DSL will report the incident and provide evidence to the police.

6.1 Power to Search, Screen, and Confiscate Devices

Under the Education Act 2011 and the Education and Inspections Act 2006, school staff have the statutory power to search, screen, and confiscate pupils' electronic devices (including mobile phones and tablets) where there is a 'good reason' to suspect a breach of school rules or risk of harm. Staff may examine files and delete data if they believe the file has been, or could be, used to disrupt teaching or break school rules. Staff will confiscate the device and hand it to the police if they suspect it contains evidence of a criminal offense.

6.2 Specific Protocol for Nude and Semi-Nude Images

In line with DfE and UK Council for Internet Safety (UKCIS) guidance, if a staff member suspects or has reasonable grounds to believe a pupil's device contains a nude, semi-nude, or sexually explicit image (youth-produced sexual imagery), the staff member must NOT view or search for the image. The device must be confiscated immediately and handed to the DSL (Ella Parker

), who will manage the incident in accordance with statutory child protection procedures and determine whether to involve the police.

7. Pupils using mobile devices (Whole-School Phone-Free Default)

To comply with statutory guidance, Meanwood is a mobile phone-free environment by default. Pupils are prohibited from using personal mobile phones, smartwatches, or interactive smart devices at any point during the school day (lessons, breaks, and lunch).

Policy Implementation Rules:

- Turn Off and Hand In: Any personal device brought to school for travel safety must be switched off completely before entering the building and handed in immediately to the class teacher.
- Secure Storage: Class teachers will store devices in a secure, designated classroom storage locker. Devices will be returned to pupils at dismissal. Devices must not be turned on until the pupil has left the school premises.
- Reasonable Adjustments (SEND/Medical): In line with the Equality Act 2010, pupils with diagnosed medical needs or complex SEND may be granted an exemption under an Individual Healthcare Plan (IHP). For example, pupils requiring a mobile app to monitor blood glucose levels (Type 1 diabetes) are permitted to have their device silent and visible on their desk. Use of this device is strictly restricted to medical tracking; any non-medical use will result in the immediate removal of the adjustment and disciplinary action.
- Sanctions: If an unhanded device is found, it will be confiscated, logged, and held securely in the school office. Parents/carers will be required to collect the device in person from the school office.

8. Staff using work devices outside school

Staff who are provided with school work devices must take all appropriate steps to ensure their security. This includes: keeping the device protected with a strong password (minimum 8 characters, with letters, numbers, and special characters), ensuring the hard drive is encrypted, setting automatic screen locking, never sharing the device with family or friends, and keeping operating systems and anti-virus software up to date. Work devices must be used solely for work activities and must never be used in any way that violates the school's acceptable use terms.

10. How the school will respond to issues of misuse

Misuse of school ICT facilities, the internet, or personal devices in a manner that impacts the school will face proportionate and immediate action. For pupils, sanctions will be applied in accordance with the Behaviour Policy. For staff, misuse will be dealt with in accordance with the staff code of conduct and disciplinary procedures. Serious incidents involving illegal content or activities will be reported to the police immediately.

11. Training

All staff members receive comprehensive online safety training during induction, with annual updates and refreshers as part of safeguarding training. The Designated Safeguarding Lead (Jo Rowlett) and deputies undergo specialized child protection and online safety training at least every 2 years, with annual knowledge updates.

Statutory Reading Mandate: All staff members must read Part One of KCSIE 2026 in full. The condensed Annex A pathway has been removed by the DfE. Training ensures that all staff are aware that technology is a key component in many safeguarding issues. Staff training covers:

- Peer-on-peer online abuse, including harassing messages and the non-consensual sharing of nude or semi-nude images.
- Online harassment, cyber-bullying, and how physical abuse and sexual violence can contain online elements.
- Spotting signs and symptoms of online abuse, grooming, and financial exploitation.
- Risks of online radicalisation, exposure to misinformation, disinformation, and conspiracy theories.
- Safe use of generative AI tools and identifying deepfakes.

12. Monitoring and Review

The DSL logs all behaviour and safeguarding issues related to online safety in the central Safeguarding File. This policy is reviewed annually by the Chair of Governors, supported by an annual digital risk assessment reflecting the rapid evolution of technology and online harms.

Appendix 1: Online safety incident report log

All online safety incidents must be recorded in this log and reported immediately to Jo Rowlett (DSL).

Date	Location of Incident	Description of Incident	Action Taken	Recorded By