



MERE SCHOOL

ONLINE SAFETY POLICY

A comprehensive safeguarding framework for managing digital safety, active filtering checks, artificial intelligence risks, and mobile-free school environments, aligned with KCSIE 2026 and Ofsted inspection baselines.

Author/Lead:	September 2024 - DR (Computing Lead)
Reviewed:	September 2026 - DR (Computing Lead)
Approved By:	Mr T Jacobs (Governor) and Mrs C Williamson (Head Teacher)
Approval Date:	September 2026
Next Review Date:	September 2027

Contents

1. Background, Scope and Rationale	3
2. Online Safety Risks and Dangers (The 4Cs)	3
3. Roles and Responsibilities in School.....	4
Head Teacher	4
Governing Body	4
Designated Safeguarding Lead (DSL) & Online Safety Lead	5
All Teaching and Support Staff	5
IT Service Provider (Oakford)	6
Learners and Parents.....	6
4. Staff Training and Online Safety Awareness.....	6
5. Mobile Phone Policy	7
6. Safer Recruitment and Volunteer Vetting	7
7. Guidance for Gender-Questioning Children	7
8. Response Protocol for AI-Generated Harm	8
9. Illegal or Inappropriate Content and Related Sanctions.....	9
10. Guidance for Reviewing Internet Sites	10
11. Relevant Legislation and References.....	10

1. Background, Scope and Rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is even truer for children, who are generally much more open to developing technologies than many adults. At home, technology is changing the way children live, and these trends are set to continue. While developing technology brings many opportunities, it also brings significant risks and potential dangers.

Scope: This Online Safety Policy outlines the commitment of Mere School to safeguard members of our school community online in accordance with statutory guidance and best practice. This policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, and community users) who have access to and are users of 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 allowed). Mere School will deal with online safety incidents within this policy and associated 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.

Associated Policies: This policy should be read in conjunction with our Safeguarding & Child Protection Policy, Anti-Bullying Policy, Positive Behaviour Policy, PSHE Policy, Staff Behaviour Policy, Acceptable Use of Technologies Policy, Computing Policy, Equality Policy, and Tackling Extremism and Radicalisation Policy.

2. Online Safety Risks and Dangers (The 4Cs)

The breadth of issues classified within online safety is considerable and ever-evolving. To ensure robust risk management, Mere School categorises online harms into the **4Cs framework** as defined by **Keeping Children Safe in Education (KCSIE) 2026**:

- **Content (Exposure to Harm):** Being exposed to illegal, inappropriate, or harmful content. This includes pornography, racism, misogyny, misandry, self-harm, suicide, antisemitism, radicalisation, extremism, extreme physical or sexual violence, and synthetic misinformation, disinformation (fake news), or conspiracy theories. This explicitly covers any exposure to AI-generated or altered suggestive materials.
- **Contact (Harmful Interaction):** Being subjected to harmful online interaction with other users or generative AI applications that simulate human interaction. This includes peer-to-peer pressure, commercial advertising, and adults posing as children/young adults with the intention to groom, manipulate, or exploit them for sexual, criminal, financial, or other purposes.
- **Conduct (Online Behaviour):** Personal online behaviour that increases the likelihood of, or causes, harm. This includes making, sending, and receiving explicit, nude, or semi-nude images (including those digitally altered or wholly generated using Artificial Intelligence or 'deepfakes'), cyberbullying, harassment, and the distribution of abusive or offensive material.
- **Commerce (Financial Harm):** Exposure to commercial risks, including online gambling, inappropriate advertising, phishing, identity theft, and online financial scams. If pupils,

students, or staff are suspected to be at risk of commercial scams, the school will report it to the IT Service Provider (Oakford).

Nudes and Semi-Nudes (KCSIE 2026 Clarification): In line with the 2026 guidance, the term 'making or sharing nudes and semi-nudes' refers to the creation, sending, or posting of nude or semi-nude images (still, moving, or livestreams) by young people under 18. This applies regardless of whether the imagery is self-generated, taken by others, or digitally altered or wholly generated using generative Artificial Intelligence (deepfakes). All such incidents require a safeguarding response, and staff are strictly prohibited from viewing, storing, or forwarding such illegal content.

3. Roles and Responsibilities in School

To ensure the online safeguarding of our community, all stakeholders must work together to develop safe, responsible behaviours, reporting inappropriate online activities as soon as they become apparent.

Head Teacher

The Head Teacher is responsible for ensuring the safety of the school community, fostering an active culture of safeguarding, and ensuring all statutory obligations are met. Day-to-day responsibilities are delegated as appropriate, but the Head Teacher retains ultimate accountability. Under KCSIE 2026, the Head Teacher must:

- Ensure the DSL/Online Safety Lead, IT technician, and relevant staff carry out their responsibilities effectively and receive suitable, regularly updated training.
- Establish an internal system to monitor and support staff who carry out online safety roles.
- Receive regular monitoring reports and incident logs from the Designated Safeguarding Lead.
- Work collaboratively with the responsible Governor, the DSL, and IT service providers (Oakford) on all aspects of filtering and monitoring.
- Joint Annual Safeguarding Audit: Jointly conduct, test, and formally record an annual review of the effectiveness of the filtering and monitoring systems alongside the DSL and IT provider (Oakford).

Governing Body

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. Governors will:

- Maintain regular meetings with the DSL and Online Safety Lead.
- Support and approve policy reviews where required.
- Ensure that the provision outlined (training, curriculum, support) is taking place as intended.
- Review online safety incident logs and challenge leaders on the effectiveness of actions taken.
- Ensure the school involves appropriate external agencies (Prevent, Police, LADO, Children's Services) if criminal or severely harmful material is discovered.

Designated Safeguarding Lead (DSL) & Online Safety Lead

Our Computing Subject Leader is responsible to the Head Teacher and Governors for day-to-day issues relating to online safety. The DSL has lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems in place). This role is explicit in their job description, and the DSL will:

- Act as a source of support, advice, and expertise for all staff on digital safeguarding.
- Receive notifications from the South West Grid for Learning, take responsibility for online safety issues, and report regularly to the Head Teacher.
- Review the school's online safety policies and practices in line with new guidance and emerging technologies.
- Ensure that all staff are aware of the specific procedures to follow in the event of an online safety incident.
- Provide training and advice for staff and induct new staff on the acceptable use of ICT.
- Liaise with class teachers to ensure that the online safety curriculum is planned, mapped, embedded, and evaluated across all year groups.
- Liaise with the Local Authority, IT technician (Oakford), and other external agencies.
- Attend relevant meetings of the Governing Body and report incident logs and actions taken.
- Retain lead responsibility for directing the IT technician to block/unblock internet sites or users.
- Maintain detailed logs of any occasions where the school has used its powers of search and deletion of data on electronic devices.

All Teaching and Support Staff

All teaching, administrative, support, premises, and catering staff are responsible for ensuring that:

- They maintain an active awareness of current online safety trends and the current school Online Safety Policy and practices.
- They understand that online safety is a core, non-negotiable part of safeguarding.
- They read, understand, and sign the staff acceptable use agreement annually.
- They immediately report any suspected misuse, technological bypass (VPN), or digital safeguarding concern to the Head Teacher, Catriona Williamson, or the DSL for investigation and action.
- All digital communications with learners and parents/carers are kept on a strictly professional level and carried out solely using official school systems (Outlook).
- Online safety is actively embedded across the curriculum, including during assemblies and daily classroom technology use.
- Learners are supervised and monitored during the use of digital technologies, and are guided only to pre-checked, age-appropriate online sites.
- They model safe, responsible, and professional online behaviours, including in their personal use of social media and outside of school.

- KCSIE 2026 Core Staff Duty: All school staff—including those who do not work directly with children, such as administrative, catering, premises, or lunchtime staff—must read, understand, and apply Part One of Keeping Children Safe in Education 2026.

IT Service Provider (Oakford)

The IT Technician (representing our service provider, Oakford) is responsible for ensuring that:

- The school's technical infrastructure is secure and protected from misuse, malicious attack, or unauthorized access.
- The school meets the technical specifications outlined in the DfE 'Meeting Digital and Technology Standards in Schools & Colleges'.
- Clear, safe, and managed control of user access is implemented across all networks.
- Network activity is regularly monitored so that any attempt to bypass systems (e.g., using VPNs or proxy sites) is identified and reported to the Head Teacher and DSL.
- The filtering policy is applied, updated regularly, and configured to send automatic alerts to the SLT and DSL.
- Active Filtering checks are maintained, and the IT technician actively participates in and supports the joint annual SLT-DSL-Oakford review of filtering effectiveness.

Pupils and Parents

Pupils must use school digital systems in accordance with their signed Acceptable Use Agreements, report any concerning content or contact immediately, and understand how to keep themselves safe. This will be logged by a member of staff in the Online Safety Log. Parents and carers play a crucial role by reinforcing online safety messages at home, acknowledging RUP agreements with a signature, and participating in the school's annual internet safety workshops run by visiting experts.

4. Staff Training and Online Safety Awareness

At Mere School, safeguarding training is integrated, aligned, and considered as part of our whole-school safeguarding approach. All staff, including non-instructional staff, undergo robust safeguarding and child protection training (including online safety and filtering/monitoring pathways) during their induction. This training is updated regularly, with all staff receiving digital safety updates at least annually (via e-bulletins, staff meetings, or briefings).

For the 2026-27 academic year, staff training pathways explicitly incorporate:

- Technical Bypasses: Identifying how pupils bypass school Wi-Fi and filtering systems using Virtual Private Networks (VPNs), proxy sites, or personal mobile data.
- Alert Workflows: Understanding how our network monitoring system flags high-risk searches and who receives these system alerts.
- Generative AI Safeguarding: Staff are only permitted to use Microsoft Office Co-Pilot and are trained not to input pupil information. Staff and pupils receive regular training including an annual Online Safety Day with Karl Hopwood.

- **Professional Boundaries:** Maintaining appropriate digital boundaries on personal messaging apps and implementing basic cybersecurity hygiene.

5. Mobile Phone Policy

Pupils' Mobile Devices: In accordance with the **2026 DfE statutory directive on Mobile Phones in Schools**, Mere School is a mobile phone-free environment by default throughout the school day. Pupils are not permitted to bring personal mobile phones or handheld devices into school. Exceptions are made solely for pupils in Years 5 and 6 who walk to and from school independently; however, these devices must be handed to their class teacher immediately upon arrival, who will lock them in the classroom drawer until the end of the school day. The SLT ensures that full records are kept of any incidents involving mobile phones or electronic devices, and these logs are reviewed by the Head Teacher and Governors on a termly basis.

Staff Personal Devices: Members of staff are permitted to bring personal mobile devices into school for professional communication. All such devices must have a locked screen and a password. Staff may only access their personal mobile devices in designated school places where pupils are **not permitted** (e.g., the staff room or teacher cupboard). Staff must never capture digital images of pupils using personal equipment; only school-owned devices (such as school iPads) may be used for educational documentation.

6. Safer Recruitment and Volunteer Vetting

Mere School operates robust recruitment and vetting procedures to prevent unsuitable individuals from working or volunteering with children. All pre-appointment checks (identity, right to work, qualifications, and enhanced DBS) are completed strictly prior to any offer of employment.

Removal of the Volunteer Supervision Exemption (Crime and Policing Act 2026): Under the latest statutory standards, the historic 'supervision exemption' for volunteers has been formally removed. Consequently, any volunteer who undertakes teaching, training, instructing, or supervising children frequently (defined as more than 3 days in a 30-day period) or overnight is deemed to be in **regulated activity**. The school **must** obtain an Enhanced DBS check with Children's Barred List information for all such regular volunteers. A written risk assessment must be completed and recorded for any volunteer not in regulated activity, and under no circumstances will a volunteer on whom no checks have been obtained be left unsupervised with children.

7. Guidance for Gender-Questioning Children

In line with the statutory expectations of **KCSIE 2026**, Mere School takes a safeguarding-first, careful, and case-by-case approach when responding to requests from children or parents regarding social transition (including requests to change pronouns, names, or uniforms). The guiding principles are as follows:

- **Safeguarding and Best Interests:** The first step in considering any social transition request is to evaluate what is in the best interest of the child and other children. School decisions may not

always align with a child's wishes, and support for social transition in primary-aged children is expected to be agreed only in exceptionally rare circumstances.

- **Parental Involvement:** Parents and carers have the leading role in their children's lives. The school will engage parents and carers as a matter of priority when a child makes a request. In rare circumstances where involving parents would constitute a direct risk to the child, the DSL must be involved to determine the appropriate safeguarding course of action before any decisions are made.
- **Physical Boundary Restrictions (Non-Negotiable):** To comply with our distinct legal and safeguarding duties under the School Premises (England) Regulations 2012 the children must not be allowed into toilets, changing rooms, or residential accommodation designated for the opposite biological sex, with no exceptions. The school must provide separate toilets for boys and girls aged 8 and over. If a gender-questioning child does not wish to use single-sex facilities designated for their biological sex, the school will consider providing a separate, self-contained individual toilet to protect the safety, comfort, privacy, and dignity of all children.
- **Digital Transition Requests:** Any digital transition requests (such as altering a pupil's name, email, or digital profile within SIMS, Insight, or Purple Mash) must be immediately referred to the DSL. These requests will be assessed strictly through the KCSIE safeguarding lens, and no digital modifications will be made without formal DSL approval and recorded parental consent.

8. Response Protocol for AI-Generated Harm

Generative AI technologies make it possible to create highly convincing fake images (deepfakes), synthetic videos, and voice clones in seconds. These tools create significant new safeguarding challenges, particularly around the non-consensual creation and distribution of suggestive or explicit synthetic images. Mere School has established a strict, written **Response Protocol for AI-Generated Harm** that all staff must follow if they suspect synthetic abuse or if a pupil makes a disclosure:

- **Isolate the Device:** If a device (such as a school computer or a confiscated personal device) is identified as containing or displaying the alleged synthetic image or video, isolate the device immediately. Do not shut it down or modify its state, as this may destroy critical digital evidence.
- **Do Not Share or Forward:** Staff must strictly NEVER share, forward, or distribute the image or video to any other person, colleague, or system, even for the purposes of investigation. Distributing or forwarding such images of a child under 18 is a serious criminal offence, regardless of whether the image is authentic or AI-generated.
- **Do Not Ask to See:** Staff must never ask to see the image, inspect the child's device privately, or search for the content on social media. They must not attempt to verify its authenticity independently.
- **Report Immediately to the DSL:** Staff must immediately report the concern to the Designated Safeguarding Lead (DSL). The DSL will take lead responsibility for logging the details (including the URL, if applicable, and describing the nature of the content), coordinating with local

authority safeguarding partners, contacting parents, and referring the matter to the Police and the Internet Watch Foundation (IWF) to secure the content's removal.

9. Illegal or Inappropriate Content and Related Sanctions

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

Category of Material / Activity	Immediate Referrals	Internal Sanctions
Child sexual abuse images (CSAM)	• Police • Children's Services	• School disciplinary / suspension
Grooming, 'sexting', or sexual incitement	• Police • Children's Services	• School disciplinary / suspension
Possession of extreme pornographic images	• Police	• School disciplinary / suspension
Criminally racist material / Hate speech	• Police • Prevent / Counter Terrorism	• School disciplinary
Pornography or sexually suggestive materials	• DSL review	• Positive Behaviour Policy / Staff disciplinary
Promotion of discrimination	• DSL review	• Consult Equality Policy / Disciplinary
Promotion of racial/religious hatred / Extremism	• Police • Prevent / CT Unit	• Positive Behaviour Policy / Disciplinary
AI-Generated Harm & Deepfakes (Suggestive/explicit images or synthetic cyberbullying)	• Police • DSL Review • IWF (for removal)	• Strict behavioral sanctions / Permanent exclusion option
Bypassing school safeguards (VPNs, proxy sites)	• IT Lead / DSL	• Confiscation / Parent contact / Positive Behaviour Policy

10. Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services (such as cyber-bullying, harassment, or deception). If you suspect that the website or device contains child abuse images (CSAM), do not follow this procedure. Halt immediately, isolate the machine, and contact the Police.

Where no illegal content is initially suspected, the following investigative procedure should be followed:

Step 1: Collaborative Process: Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

Step 2: Designated Hardware: Conduct the procedure using a designated computer that will not be used by young people and, if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

Step 3: Monitored Access: Ensure that the investigating staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

Step 4: Record the Evidence: Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used. These should be printed, signed, and attached to the incident file (except in the case of child sexual abuse images).

Step 5: Formulate Judgement: Once the investigation is complete, the senior staff group must judge whether the concern has substance. If it does, they must initiate appropriate action (internal disciplinary response, local authority/MAT escalation, or police referral).

11. Relevant Legislation and References

This policy is established upon the statutory baselines and provisions of the following primary legislation and departmental guidance:

- DfE Keeping Children Safe in Education (2026 statutory guidance)
- DfE Teaching Online Safety in Schools (2023 departmental advice)
- DfE Mobile Phones in Schools (2024 statutory guidance / 2026 default standard)
- DfE Searching, Screening and Confiscation (2022 advice for schools)
- The Crime and Policing Act 2026 (removal of supervision exemptions for volunteers)
- The Data (Use and Access) Act 2025 (effective January 2026, updating UK data laws)
- The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)
- The Human Rights Act 1998 and Equality Act 2010 (including the Public Sector Equality Duty)
- UK Council for Child Internet Safety (2020) Education for a Connected World framework
- The Computer Misuse Act 1990 and Voyeurism (Offences) Act 2019