Sir John Lillie Primary School
Online safety policy

	Designated Safeguarding Lead (DSL) team	Sue Hayward
	Online-safety lead	Pedro Lima
	Online-safety / safeguarding link governor	Sue Hardwick
	PSHE/RSHE lead	Victoria Hall/ Chloe Grassie
	Network manager / other technical support	Strictly Education

Contents

1. Aims

Our school aims to:

- Implement Robust Safeguarding: Maintain dynamic filtering and monitoring systems alongside clear procedural frameworks to ensure the online safety of pupils, staff, volunteers, and governors.
- Foster Digital Resilience: Deliver a progressive curriculum that empowers the whole school community to use technology critically, ethically, and safely—moving beyond "avoidance" to active risk management.
- Ensure Rapid Intervention: Establish transparent mechanisms to identify, document, and escalate online incidents (including cyberbullying and peer-on-peer abuse), ensuring swift support for those affected.
- Bridge the Home-School Gap: Work in active partnership with parents and carers to provide consistent guidance and support regarding children's digital lives outside of the classroom.
- Adapt to Emerging Tech: Proactively address the challenges and opportunities of new technologies, including Generative AI, ensuring that data privacy and academic integrity are maintained.

2. Legislation and Guidance

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

- **Teaching Online Safety in Schools:** Integrating safety into the curriculum.
- **Filtering and Monitoring Standards for Schools:** Meeting the technical requirements to protect pupils from harmful content on school networks.
- **Preventing and Tackling Bullying:** Specific advice on cyber-bullying and peer-on-peer abuse.
- **Relationships, Sex and Health Education (RSHE):** Guidance on healthy digital relationships and the risks of online exploitation.
- **Searching, Screening and Confiscation:** Advice for schools on handling electronic devices.
- **Prevent Duty:** Protecting children from radicalisation and extremist content online.

Legal Framework

This policy reflects existing legislation, including but not limited to:

- **The Online Safety Act 2023:** Which mandates a higher duty of care for platforms and informs school risk assessments regarding harmful content.
- **The Data Protection Act 2018 and UK GDPR:** Governing the use of pupils' personal data and images.
- **The Education Act 2011:** Granting teachers the power to search for and delete inappropriate material on electronic devices where there is a "good reason" to do so.
- **The Equality Act 2010:** Ensuring protection for all pupils, particularly those vulnerable to online hate speech or harassment.

The policy also aligns with the **National Curriculum computing programmes of study**, specifically regarding "Online Safety" and "Digital Literacy" outcomes.

3. Roles and Responsibilities

3.1 Headteacher

Key responsibilities:

- **Strategic Oversight of Filtering and Monitoring:** Ensure the school meets the DfE Digital and Technology Standards by reviewing filtering and monitoring reports at least termly. The Headteacher must be able to explain how these systems work and how they protect against the "Four Cs" (Content, Contact, Conduct, and Commerce).
- **Culture of Digital Safety:** Foster a culture where online safety is not a "one-off" lesson but is fully integrated into the whole-school safeguarding approach, ensuring staff treat online harms with the same severity as offline harms.
- **Mobile Phone Policy Enforcement:** Implement and consistently enforce the school's policy on mobile technology, ensuring it is clearly communicated to parents and pupils.
- **AI and Emerging Technology Risks:** Oversee the school's response to emerging risks, including **Generative AI (e.g., deepfakes, misinformation)**, ensuring that AI-related safeguarding risks are included in school risk assessments.
- **Training & Staff Competency:** Ensure all staff receive annual online safety training that includes the latest risks (e.g., radicalisation, online sexual exploitation, and cybersecurity) and that this is part of the induction for all new staff.
- **Data Management & Privacy:** Take overall responsibility for data management and UK GDPR compliance, working with the DPO to ensure that data protection processes support legal information sharing without compromising child protection.
- **Incident Response:** Maintain and communicate clear procedures for staff to follow in the event of a serious online safeguarding incident or cyber-attack, ensuring a coordinated response between IT staff and the safeguarding team.
- **Curriculum Quality:** Ensure that the online safety curriculum is broad and balanced, covering digital resilience, critical evaluation of content (misinformation), and healthy online relationships.
- **Governor Reporting:** Provide regular, evidence-based updates to governors regarding the effectiveness of online safety arrangements, including any significant trends identified through monitoring logs.
- **Website Compliance:** Ensure the school website meets all statutory requirements and provides up-to-date online safety resources and reporting links for parents and pupils.

3.2 Designated Safeguarding Lead (DSL) / Online Safety Lead

Key responsibilities:

- **Lead Responsibility:** Retain lead responsibility for safeguarding and child protection, including online safety. While technical tasks may be delegated, the DSL's overarching responsibility for the safety of the digital environment cannot be delegated (KCSIE).
- **Active Filtering & Monitoring (F&M) Management:** Take ownership of the school's "Filtering and Monitoring" systems. This includes:
    - Conducting at least **annual reviews** of filtering logs and monitoring alerts.
    - Ensuring the system effectively blocks the "Four Cs" (Content, Contact, Conduct, and Commerce).
    - Working with IT staff to ensure alerts are handled with the same urgency as face-to-face disclosures.
- **AI Risk Assessment:** Lead the school's assessment of risks associated with **Generative AI**, including its potential for creating non-consensual imagery, facilitating plagiarism, or exposing children to biased/age-inappropriate algorithms.

- **Multi-Agency Liaison:** Liaise with pastoral staff, IT technicians, SENCOs, and Senior Mental Health Leads. Ensure that online incidents are viewed through a "trauma-informed" lens, recognizing the impact of digital harm on a pupil's mental health.
- **Curriculum & Resilience:** Ensure online safety education is embedded across the curriculum (not just in Computing or RSHE). This must include teaching pupils how to critically evaluate **misinformation, "fake news," and AI-generated content.**
- **Parental Engagement (Digital Partnership):** Proactively support parents and carers, including "hard-to-reach" families, by providing guidance on home filtering, age-appropriate gaming, and social media trends.
- **Incident Logging & Analysis:** Ensure all online safety incidents are logged via the school's safeguarding software (CPOMs).
- **Data Privacy & Ethics:** Work with the Headteacher and DPO to ensure a GDPR-compliant framework. Ensure that any third-party educational software or AI tools used in school have undergone a **Data Protection Impact Assessment (DPIA)**.
- **Staff Training & Empowerment:** Facilitate annual training for all staff (including supply teachers and volunteers). Ensure all staff have read and understood **KCSIE Part 1 and Annex C (Online Safety)**. Provide specific "cascade" training on new apps or platforms trending among the pupils.
- **Reporting Mechanisms:** Maintain clear, accessible pathways for pupils to report concerns, such as a "Whisper" button or a "Something is worrying me" link on the school homepage, ensuring these are monitored during school holidays or remote learning periods.
- **Mobile & Wearable Tech:** Oversee the implementation of the school's policy on personal devices (including smartwatches), ensuring a "safe and focused" learning environment in line with **DfE directives.**

3.3 Governing Body, led by Online Safety / Safeguarding Link Governor

Key responsibilities:

- **Statutory Accountability:** Take overall responsibility for ensuring the school meets its statutory duties regarding online safety, specifically ensuring the school's filtering and monitoring systems are effective and regularly reviewed.
- **Strategic Challenge of Technical Standards:** Work with the Headteacher and DSL to ensure the school meets the **DfE Digital and Technology Standards**. This includes asking for evidence that:
    - Filtering and monitoring systems are "checked" at least annually.
    - The system is blocking harmful content while allowing "safe failure" (educational access).
- **Integrated Safeguarding Oversight:** Ensure that online safety is a standing item in safeguarding reports and governor meetings, treating digital harms with the same priority as physical safeguarding.
- **Policy & Compliance Review:** Regularly review and approve the Online Safety Policy and **Acceptable Use Policies (AUPs)**, ensuring they reflect current 2026 trends such as Generative AI risks and the mobile-free school environment.
- **Training Verification:** Ensure that the Governing Body itself receives up-to-date training on online safety risks (including cybersecurity and AI) to effectively hold school leaders to account.
- **Data Privacy & Ethics Oversight:** Work with the Data Protection Officer (DPO) and Headteacher to ensure the school remains UK GDPR compliant, specifically scrutinizing the privacy impact of any new educational software or AI integration.
- **Community Engagement:** Support the school in building strong digital partnerships with parents and the local community, ensuring that online safety messages are consistent beyond the school gates.
- **Cyber Recovery Planning:** Ensure the school has a robust **Cyber Incident Response Plan** and that governors are aware of their role in the event of a significant data breach or system failure.

3.4 All Staff

Key responsibilities:

- **Human Oversight:** Recognise that while technical filters (Filtering & Monitoring) are in place, they are not infallible. Staff must provide active, "human oversight" whenever pupils are using devices, looking for signs of distress or engagement with inappropriate content that technology may miss.
- **Proactive Reporting:** Record and report all online-safety incidents—including cyberbullying, exposure to harmful AI content, and "low-level" digital concerns with the same urgency as physical safeguarding issues.
- **Filtering and Monitoring Awareness:** Understand how the school's filtering and monitoring systems work. Staff must know how to report "over-blocking" (which hinders learning) or "under-blocking" (where harmful content is accessed) immediately to the DSL.
- **AI Literacy & Ethics:** Be aware of the risks posed by **Generative AI**, including its ability to create believable misinformation, "fake news," and non-consensual deepfake imagery. Staff should model the critical evaluation of AI-generated resources before use in the classroom.
- **Digital Resilience in the Curriculum:** Identify opportunities to "thread" online safety through all subjects. This includes teaching pupils to question the digital "jigsaw puzzle"—helping them spot manipulation, extremist narratives, and online grooming.
- **Data Privacy & Security:** Maintain high standards of "cyber hygiene," including the use of strong passwords and Multi-Factor Authentication (MFA). Staff must ensure that any new app or AI tool has been vetted for GDPR compliance by the DSL/DPO before being introduced to pupils.
- **Professional Conduct & Modelling:** Model safe, responsible, and professional behaviour in all digital interactions. This includes maintaining professional boundaries on social media and ensuring that personal digital footprints uphold the reputation of the school and the profession.
- **Remote & Hybrid Learning:** When supporting pupils via remote platforms, follow the school's specific safeguarding principles for online lessons, ensuring that the same high standards of behaviour and "Safe Search" expectations apply as they do in the physical classroom.
- **Zero-Tolerance to Digital Harassment:** Take a zero-tolerance approach to online sexual harassment and the sharing of indecent images, ensuring that any such incident is treated as a serious safeguarding breach rather than just a "behaviour" issue.

3.5 PSHE / RSHE Lead/s

Key responsibilities (in addition to the "all staff" section):

- **Statutory Curriculum Alignment:** Lead the transition to the **RSHE statutory requirements**, ensuring the curriculum explicitly addresses:
    - **AI and Deception:** Teaching pupils to recognize AI-generated content, fake profiles, and the risks of "emotional simulation" in chatbots.
    - **Digital Wellbeing:** Addressing the impact of algorithms, endless scrolling, and social media on mental health, body image, and self-worth.
    - **Online Misogyny and Subcultures:** Tackling harmful online ideologies, gender stereotypes, and "influencer" culture in an age-appropriate way.
- **Consent & Digital Boundaries:** Embed a modern understanding of consent that covers the digital space—including the ethics of sharing images, the impact of non-consensual deepfakes, and respecting "digital personal space."
- **Critical Media Literacy:** Work with the Computing Lead to ensure pupils can distinguish between fact, opinion, and **misinformation/conspiracy theories**, as now mandated by KCSIE.
- **Financial Exploitation Education:** Integrate lessons on online financial harms, including "loot boxes" in gaming, in-app purchases, and the psychology of digital scams/fraud.
- **Inclusive Education:** Ensure RSHE remains inclusive and trauma-informed, reflecting diverse family structures and protecting pupils from online hate speech or harassment based on protected characteristics.
- **Parental Transparency:** Maintain the school's RSHE policy on the website and ensure all RSHE teaching materials are available for parental review upon request.
- **Cross-Curricular Mapping:** Coordinate with the Computing Lead to ensure a "no-gaps" approach: while Computing focuses on technical security and "how it works," PSHE focuses on "how it feels" and the human impact of online interactions.

3.6 Computing Lead

Key responsibilities (in addition to the "all staff" section):

- **AI Literacy Curriculum:** Lead the integration of **Generative AI literacy** into the Computing curriculum, ensuring pupils understand how Large Language Models (LLMs) work, the risks of "hallucinations" (false info), and the ethics of AI-generated content.
- **Critical Media Evaluation:** Direct the teaching of advanced search and verification skills, specifically how to identify "deepfakes," manipulated media, and bot-driven engagement.
- **Technical Safeguarding Liaison:** Collaborate with technical staff (ICT Manager) to ensure that the school's infrastructure (filtering/monitoring) supports the curriculum without being so restrictive that pupils cannot learn to navigate risk safely.
- **Data Privacy & Security Education:** Oversee the teaching of robust "cyber-hygiene," including the importance of **Multi-Factor Authentication (MFA)**, the risks of "Internet of Things" (IoT) devices, and an age-appropriate understanding of data harvesting.
- **RSHE Coordination:** Work in a "no-gaps" partnership with the RSHE Lead. While RSHE covers healthy online relationships, the Computing Lead must ensure the technical mechanics of those platforms (algorithms, privacy settings, and reporting buttons) are understood.
- **Review of EdTech Tools:** Conduct (or assist with) **Data Protection Impact Assessments (DPIAs)** for any new educational software or AI tools introduced in the classroom.
- **Digital Leadership:** Oversee any "Digital Lead" or "e-Safety Cadet" pupil groups, empowering them to model peer-to-peer support and safe digital habits.

3.7 Curriculum Managers

Key responsibilities (in addition to the "all staff" section):

- **Subject-Specific Online Safety Integration:** Conduct a curriculum audit to identify and embed opportunities for teaching online safety within your subject. For example:
    - **English/Literacy:** Teaching pupils to evaluate the reliability of sources and identify **misinformation, disinformation, and AI-generated "fake news."**
    - **History/Geography:** Discussing the use of propaganda and the influence of digital subcultures and algorithms on global events.
    - **Maths:** Addressing the logic behind algorithms and the financial risks of online commerce, such as **scams, "loot boxes" in gaming, and in-app purchases.**
    - **Science:** Exploring the ethics of **Artificial Intelligence** and data privacy in technology.
- **Critical Media Literacy:** Take lead responsibility for ensuring pupils are taught how to critically engage with what they see online. This includes recognizing **conspiracy theories** and understanding why a person or organization might want them to believe certain information.
- **Modelling Professional Digital Habits:** Ensure that any digital resources, videos, or AI tools used within your subject are vetted for age-appropriateness and meet the school's **Data Protection (GDPR) and Filtering standards**.
- **Action Plan Alignment:** Ensure that subject-specific action plans explicitly include an online-safety element, demonstrating how your subject contributes to the school's "whole-school approach" to digital resilience.
- **Liaison with DSL & Specialists:** Work closely with the DSL/Online Safety to ensure that the messaging in your subject aligns with the school's core safeguarding principles and latest trends.
- **Inclusive Resource Selection:** When choosing online materials, ensure they do not unintentionally reinforce harmful stereotypes or expose pupils to inappropriate "influencer" culture, particularly in light of new guidance on **online misogyny**.

3.8 Network Manager / Technical Staff

Key responsibilities (in addition to the "all staff" section):

Technical Lead for Filtering and Monitoring (F&M): * Maintain the school's filtering and monitoring systems to ensure they meet the **DfE Core Standards**.

- Ensure systems can identify the **individual, device, time, and date** of any attempted access to blocked content.
- Perform **annual technical audits** to verify that filters are blocking the "Four Cs" (Content, Contact, Conduct, Commerce) and haven't been bypassed by VPNs or unauthorized browser plugins.

Cyber Security & Resilience (Cyber Essentials):

- Implement and maintain robust **Multi-Factor Authentication (MFA)** for all staff accounts, particularly for cloud services (SaaS), email, and MIS systems, as mandated by the Cyber Essentials update.
- Maintain an up-to-date **Information Asset Register** to track all hardware.
- Execute and test a **Cyber Incident Response Plan**, ensuring "offline" or immutable backups are in place to recover from ransomware or data loss.

Safeguarding-First Architecture: * Work in a "safeguarding-first" partnership with the DSL to ensure network changes (e.g., YouTube Restricted Mode, Cloud sharing permissions) are risk-assessed before implementation.

- Provide the DSL with **interpretable F&M reports**—data must be in a format that allows non-technical safeguarding leads to identify risks urgently.

Generative AI Governance:

- Configure school devices and networks to ensure **AI tools** are accessed through safe, school-approved channels that do not harvest pupil data for training models.
- Lock "Safe Search" into all chosen browsers and prevent the download of unauthorized browsers.

Reporting & Escalation:

- Immediately report technical "red flag" alerts (e.g., attempts to access illegal content or signs of a cyber-attack) directly to the DSL and Headteacher.
- Document all "filtering change requests" to provide a clear audit trail for Governors and Ofsted.

School Website Compliance:

- Support the Headteacher in ensuring the school website remains compliant with the DfE requirements, including the publication of the latest RSHE policy and financial benchmarking links.

3.9 Data Protection Officer (DPO)

Key responsibilities:

- **Safeguarding-First Data Sharing:** Ensure all staff understand that **UK GDPR and the Data (Use and Access) Act 2025 do not prevent the sharing of information** for the purposes of keeping children safe, "Safeguarding" remains a valid legal basis for processing sensitive data without consent (DPA 2018 / DUAA 2025).
- **Robust Retention Management:** Oversee the school's retention schedule. While the standard remains "until the pupil is 25," many local authorities now mandate retention **until age 35** for child protection files to account for the Limitation Act. Files related to child sexual abuse should be retained for **75 years**.

- **Filtering and Monitoring Privacy:** Collaborate with the DSL and Network Manager to ensure that "monitoring" is proportionate. The DPO must verify that the school's surveillance of digital activity is transparent (via Privacy Notices) and respects the balance between safety and the right to privacy.
- **Cyber Incident Support:** Act as a key responder in the **Cyber Incident Response Plan**, lead on reporting any significant data breaches to the **Information Commission** (formerly the ICO) within 72 hours, and manage communications with affected families.
- **Subject Access Request (SAR) Management:** Handle SARs with a "reasonable and proportionate" search approach (as codified in the 2025 Act), while ensuring that sensitive safeguarding notes are appropriately redacted if their disclosure would place a child at risk of harm.
- **Information Sharing Records:** Ensure the school maintains a "Data Sharing Log" that records *who* information was shared with, *why*, and the legal basis (e.g., Public Task or Legitimate Interest).

3.10 LGfL TRUSTnet Nominated Contacts

Key responsibilities:

- **Service Management & Accountability:** Manage all LGfL services (including SchoolProtect, USO, and GridStore) on behalf of the school, ensuring they are configured to support the school's Online Safety and Data Protection policies.
- **Filtering & Monitoring Configuration:** Act as the primary interface for implementing the "Appropriate Filtering" levels decided by the DSL. This includes:
    - Managing block/allow lists in **SchoolProtect**.
    - Ensuring **YouTube Restricted Mode** and other content-control features are active and effective across all school-managed devices.
- **Identity & Access Management (USO):** Oversee the **Unified Sign-On (USO)** system to ensure every pupil and staff member has a personal, auditable account.
    - Enforce the school's **MFA (Multi-Factor Authentication)** requirements through LGfL's security settings.
    - Ensure accounts are promptly disabled when staff or pupils leave the school to prevent unauthorized access to sensitive data.
- **Data Handling & Privacy:** Work with the DPO to ensure that any LGfL service used for storing personal data (such as cloud backups or email) follows strict UK GDPR and **Data (Use and Access) Act 2025** procedures.
- **Safeguarding Partnership:** Hold regular reviews with the DSL and DPO to ensure they understand:
    - Exactly **who** has Nominated Contact status (typically up to 5 staff members).
    - What level of data access these individuals have.
    - The safeguarding implications of any technical changes requested (e.g., opening specific ports or unblocking social media categories).
- **Incident Support:** Use LGfL technical logs to assist the DSL in investigating online safety incidents, providing detailed evidence of search terms, access times, and blocked attempts when required for a safeguarding file.
- **Continuous Training:** Stay updated with LGfL's latest security features and "SafeguardED" updates to ensure the school is making full use of the technical protections provided by the grid.

3.11 Volunteers and Contractors

Key responsibilities:

- **AUP Compliance & Induction:** Read, understand, and sign the school's **Acceptable Use Policy (AUP)** before starting any work. This must be accompanied by a briefing from the DSL (Sue Hayward) on the school's specific digital safeguarding culture.

- **Proactive Reporting of Risks:** Report any online safety concern—regardless of how minor it seems—directly to the DSL. This specifically includes spotting signs of:

    - **Disinformation/Misinformation:** Pupils being influenced by harmful "fake news" or conspiracy theories.
    - **AI-Generated Harm:** Any mention of non-consensual deep fake imagery or harmful interactions with AI chatbots.
    - **Strict Communication Boundaries:** * **Never** contact a pupil via personal social media, private email, or messaging apps.

    - **Never** arrange any face-to-face or digital meeting (e.g., tutoring) without the explicit, documented approval of the DSL and the pupil's parents.
    - Use only school-approved platforms (e.g., LGfL/Google Workspace) for any necessary communication.

- **Modelling Professionalism:** Uphold the same standards of "digital professionalism" as permanent staff. This includes being mindful of their own digital footprint, as pupils may search for them online.
- **Awareness of New Offences:** Maintain an awareness of the legal landscape, including new criminal offences under the **Online Safety Act** such as "cyber flashing" and "encouraging serious self-harm," and understand their duty to report such behaviours.
- **Data Privacy:** Handle any pupil data (names, login details, or work) according to the school's Data Protection policy and never store pupil information on personal, unencrypted devices.

3.12 Pupils

Key responsibilities:

- **Adherence to a Phone-Free Environment:** Follow the school's "Mobile-Free" policy. This means personal devices (including smartphones and smartwatches) must be switched off and handed to the school office until the end of the school day.
- **Acceptable Use & Annual Review:** Read and follow the **Acceptable Use Policy (AUP)**. Pupils must understand that this policy applies to their behaviour both in school and outside of school (including on social media) if their actions affect the school community.
- **Critical Thinking & AI Awareness:** * Develop the skills to identify **misinformation, "fake news," and conspiracy theories**.

- Learn to recognize **AI-generated content** (e.g., deep fakes or bot-written text) and understand that AI can sometimes be biased or incorrect ("hallucinations").

- **Safe Reporting (The "Speak Up" Rule):** Know how to report any online concerns (bullying, inappropriate content, or suspicious contact) using the school's secure reporting tools (e.g., the "Whisper" button or "Help" link).

    - Understand that reporting a concern—even if it involves a friend—is a brave and responsible act.

- **Digital Boundaries & Privacy:**

    - Never use personal logins or private messaging (e.g., WhatsApp, Discord) to communicate with school staff.
    - Respect the privacy of others by never taking, sharing, or manipulating photos/videos of peers or staff without explicit permission.

- **Online Wellbeing & Resilience:** Be mindful of "screen time" and the impact of social media algorithms on their feelings. Pupils should know when to "log off" and who to talk to if they feel overwhelmed or upset by something they see online.
- **Healthy Relationships:** Treat others with the same respect online as they would in person. This includes taking a **zero-tolerance approach** to online misogyny, hate speech, and peer-on-peer digital harassment.

3.13 Parents and Carers

Key responsibilities:

- **Support the Phone-Free Environment:** Adhere to the school's Mobile-Free Policy. If a child requires a phone for the journey to/from school, parents must ensure it is handed in at the school gate as per the school's specific storage procedure.
- **Adhere to Screen Time Guidance:** Follow the DfE Parental Guidance on Screen Time, aimed at balancing digital use with physical health, sleep, and face-to-face social interaction.
- **Model "Healthy Digital Habits":** Demonstrate responsible technology use, including seeking permission before posting images of other children (sharenting) on social media.
- Refrain from using personal mobile phones in the school playground or during school events to model the school's focus on "present" social engagement.
- **Manage Home AI and Algorithms:** Monitor child interactions with Generative AI (chatbots), ensuring they understand these are not "friends" and may provide incorrect or biased information.
- Regularly check privacy settings and age-restrictions on apps like Roblox, TikTok, and YouTube, being aware that age-verification standards are now much stricter.
- **Critical Thinking Partnership:** Talk to your child about "fake news" and deepfakes. Support the school's curriculum by encouraging children to question whether what they see online is real or computer-generated.
- **Safe Remote Learning (where applicable):** Continue to provide a safe environment for any remote education, ensuring children work in communal areas (not bedrooms) and follow the "dress code" and "blurred background" protocols.
- **Vetting Private Tutors**: If hiring private online tutors, parents must verify that the tutor has a current Enhanced DBS check and agree to the school's "No Private Messaging" rule between tutors and pupils.
- **Respectful Community Conduct**: Use social media and messaging groups (e.g., WhatsApp class groups) positively. Parents must not post negative or defamatory comments about staff, pupils, or other parents, as this can undermine the school's safeguarding culture.

3.14 External Groups (including Parent Associations)

Key responsibilities:

- **Digital Agreement (AUP):** Every external individual or organization leader must sign the **External User Acceptable Use Policy** before accessing the school's network, using school devices, or conducting school-branded activities online.
- **Event Safety:** If an external group organizes a school event (e.g., a disco or fair), they must support the school's **Mobile-Free Environment** and ensure that any digital aspects of the event (like digital playlists or photo booths) are vetted by the DSL for age-appropriateness.
- **Data Protection & Privacy:** Parent associations must handle any community contact lists (e.g., for fundraising) in compliance with **UK GDPR and the Data (Use and Access) Act 2025**, ensuring data is never shared with third parties without explicit permission.
- **Modelling Respectful Behaviour:** Model the school's values of kindness and respect in all digital communications. External groups must refrain from using digital platforms to bypass school communication channels for grievances or to post negative comments about staff, governors, or other families.
- **Safeguarding Vigilance:** Report any "low-level" safeguarding concerns that arise during community events or within parent-led digital groups directly to the **DSL or Deputy DSL**

4. Educating Pupils about Online Safety

The school will deliver a progressive online safety curriculum that is integrated into **Computing**, **RSHE**, and other subjects where relevant. This curriculum is based on the **"Education for a Connected World"** framework.

In Key Stage 1, pupils will be taught to:

- **Digital Privacy:** Understand what "personal information" is and why it must be kept private (e.g., full name, school name, and home address).
- **Safe Communication:** Use technology safely and respectfully, understanding that there is a "real person" behind the screen.
- **The "Help" Rule:** Identify trusted adults (at home and school) to go to if they feel worried, uncomfortable, or see something "strange" online.
- **Foundational AI Literacy:** Understand that some "toys" and apps use AI to talk or react, and that these are computer programs, not real people.

In Key Stage 2, pupils will be taught to:

- **Critical Evaluation (The "Seeing is Not Believing" Rule):** * Recognize that information online can be biased, incorrect, or intentionally misleading (**misinformation/disinformation**).
    - Understand how **AI and Deepfakes** can create realistic but "fake" images, videos, and voices.
- **Algorithmic Awareness:** Develop a basic understanding of how apps use "algorithms" to show them more of what they like, and how this can affect their feelings and time spent online.
- **Healthy Digital Relationships:** * Recognise acceptable and unacceptable behaviour (including **online misogyny** and **cyberbullying**).

    - Understand that "anonymity" does not excuse poor behaviour.

- **Technical Resilience:** Use search technologies effectively and understand how results are selected and ranked.
- **AI Ethics & Capabilities:** * Develop an understanding of AI's capabilities (e.g., generating text/art) and its limitations (e.g., making mistakes or "hallucinations").

    - Learn to use AI tools responsibly as a "creative partner" rather than a "source of truth."

By the end of primary school, pupils will know:

- **The Four Cs of Risk:** How to identify risks related to **Content** (harmful images/news), **Contact** (grooming/scams), **Conduct** (bullying), and **Commerce** (gaming "loot boxes" and financial scams).
- **The Impact of Digital Footprints:** That what is posted online can be seen by others and may stay there "forever," impacting their future reputation.
- **Online/Offline Balance:** How to manage "screen time" and recognize when digital use is affecting their sleep, mood, or physical health.
- **Location Safety:** The importance of keeping location settings "off" on devices and apps to protect their physical safety.

Delivery and Awareness

- **Cross-Curricular Threading:** Online safety will be "threaded" through English (evaluating sources), Maths (data and algorithms), and Science (AI ethics).
- **Whole-School Events:** The school will celebrate **Safer Internet Day** annually and hold regular assemblies to address emerging trends (e.g., new gaming platforms or viral challenges).
- **Reporting Mechanisms:** All pupils will be regularly reminded of how to use the school's internal reporting tools and external support services like **Childline** and **CEOP**.

5. Educating Parents about Online Safety

The school recognizes that a "whole-school approach" to safety must include a robust partnership with parents. We aim to move beyond "scare tactics" toward empowering families with digital resilience.

Communication and Resources

- **The "Drip-Feed" Approach:** Instead of annual workshops, the school will provide monthly "bite-sized" updates via the school newsletter and website. These will cover emerging trends such as:
    - **AI and Deepfakes:** Helping parents understand that AI-generated content (including "undressing" apps or voice cloning) is a risk even for primary-aged children.
    - **Algorithmic Influence:** Explaining how "infinite scroll" and "recommended" feeds on platforms like YouTube Kids or TikTok can affect a child's mood and sleep.
    - **Gaming Monetization:** Advice on "loot boxes," in-app purchases, and the risks of "commerce" in popular games like Roblox.

Engagement and Support

- **Signposting Trusted Help:** Our website will maintain a dedicated "Parent Advice & Help – Online Safety" page linking to resources from:
    - **Internet Matters:** For device-specific setup guides.
    - **NSPCC / Childline:** For advice on starting "awkward" conversations about online behavior.
    - **Report Remove (IWF):** For urgent help if a child's image has been shared online.

Reporting Concerns

- **First Point of Contact:** If parents have any concerns about their own child's digital safety or the behaviour of others online, they should contact the **Headteacher/DSL/Deputy DSL**
- **Policy Feedback:** We welcome parental input on this policy. Any queries regarding the school's digital approach can be raised with any member of staff.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps, or gaming sites. This definition explicitly includes:

- **AI-Generated Abuse:** The use of Generative AI to create fake images, "nudification" of photos (**deepfakes**), or manipulated audio/video of pupils or staff.
- **Algorithmic Harassment:** The intentional "piling on" or use of bots to harass an individual.
- **Intimate Image Abuse:** The sharing or threatening to share private or manipulated images (a priority offence under the Online Safety Act).

6.2 Preventing and Addressing Cyber-bullying

To help prevent cyber-bullying, the school will foster a culture of **Digital Resilience**:

- **Critical Media Literacy:** Pupils are taught to recognize that online content (including AI images) can be faked or manipulated to cause harm.
- **The "Bystander to Upstander" Rule:** Pupils are encouraged to report abuse they witness; not just abuse they experience.
- **Targeted Curriculum:** Cyber-bullying is addressed through the RSHE and Computing curriculum, with a specific focus on the **"Four Cs"** of risk (Content, Contact, Conduct, and Commerce).

- **Restorative Practice:** Where appropriate, the school will use restorative education modules to help perpetrators understand the real-world impact of digital harm.

6.3 Examining Electronic Devices (Search & Confiscation)

Under the **DfE Guidance**, schools are expected to be **mobile-phone-free environments**. Mobile phones are not permitted to be used during the school day.

Staff Powers to Search: School staff have the power to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices where they have a "good reason."

- **Reasonable Suspicion:** Staff may search a device if they suspect it contains material that could cause harm, disrupt teaching, or break school rules (including the ban on phone use).
- **AI & Illegal Content:** If a staff member suspects a device contains **AI-generated illegal content** (such as non-consensual deepfakes) or "Priority Harm" content (e.g., self-harm encouragement), the device must be seized and the **DSL /Deputy DSL** informed immediately.

The Examination Process:

- **Safeguarding First:** If staff suspect the device contains **indecent images of a child**, they must **not** view the images. They must secure the device and hand it to the DSL, who will contact the police.
- **Parental Presence:** While staff have the legal power to search, it is school policy to contact parents to seek permission and invite them to be present during the examination of a device, unless doing so would place a child at risk of harm.
- **Data Erasure:** Staff may only delete files if there is a "good reason"—for example, to stop the further spread of a harmful image among the school community. This must be documented in the school's safeguarding system.

7. Acceptable Use of the Internet in School

All staff, volunteers, and governors are required to sign an **Acceptable Use Policy (AUP)** annually. These agreements explicitly cover the safe use of **Generative AI** and the enforcement of **phone-free school sites**.

7.1 General Principles

- **Educational Purpose:** Use of the school's internet and ICT systems must be for educational purposes or for fulfilling the specific duties of an individual's role. Personal browsing is permitted only within the strict boundaries defined in the Staff Code of Conduct.
- **Accountability:** Every user will access the network through an individual, password-protected account. Sharing of logins is a significant security breach and is strictly prohibited.
- **Prohibited Material:** Users must not intentionally visit, download, or share material that is obscene, violent, illegal, hateful, or otherwise objectionable. This includes the use of AI to generate such content.

7.2 Filtering and Monitoring (DfE Standards)

The school employs an active, multi-layered filtering and monitoring system that meets the **DfE Core Standards**:

- **Filtering:** Our system (e.g., LGfL SchoolProtect) blocks access to harmful content across the "Four Cs" (Content, Contact, Conduct, and Commerce). This includes the blocking of unauthorized VPNs and "bypass" tools.
- **Monitoring:** User activity on all school devices (and any personal devices connected to school Wi-Fi) is monitored. Our system provides **urgent alerts** to the DSL for "red flag" search terms or activities.
- **Annual Reviews:** The DSL and a nominated Governor will conduct an annual review of the filtering and monitoring logs to ensure the system is age-appropriate and effective for our school's specific risk profile.

7.3 Use of Generative AI

- **Staff Use:** Staff may use school-approved AI tools to support lesson planning and administration, provided no sensitive pupil data is entered into the prompts (unless the tool has undergone a Data Protection Impact Assessment).
- **Pupil Use:** Pupils will only use AI tools under the direct supervision of a teacher. They are taught that AI-generated content must be critically evaluated and should not be presented as their own original work without proper citation.

7.4 Network Security and Cyber-Hygiene

- **MFA (Multi-Factor Authentication):** All staff and governors must use MFA to access cloud services (e.g., Google Workspace/Office 365) and any systems containing pupil data.
- **Unauthorised Software:** Users are not permitted to install software or "browser extensions" on school devices without approval from the Network Manager.
- **Data Security:** Personal or sensitive data must only be stored in school-approved cloud locations and never on personal, unencrypted USB sticks or hard drives.

8. Pupils using mobile devices in school

8.1 The "Phone-Free" School Environment

In line with the **DfE mandate**, this school is a mobile-phone-free environment. This is to ensure a calm, safe, and focused atmosphere, protecting pupils from the distractions and safeguarding risks (such as cyber-bullying and access to inappropriate content) associated with personal devices.

8.2 Year 5 and 6 Protocol

We recognize that some parents may wish their children in Year 5 and 6 to carry a mobile phone for safety while traveling to and from school independently.

- **Storage:** Any mobile device brought into school must be switched off at the school gate and handed directly to the school office/class teacher and signed in upon arrival.
- **Security:** Devices will be stored in a secure, locked location (e.g., the school office) and will not be accessible to pupils at any point during the school day, including lunch and break times.
- **Collection:** Phones may be collected at the end of the school day and signed out by pupils.
- **Emergency Use:** If a pupil needs to contact home during the day, they must do so via the school office.

8.3 Recommended Device Type

In line with the **"Smartphone-Free Childhood"** movement and DfE recommendations, we strongly encourage parents to provide children with a **basic "brick" phone** (calls/texts only) rather than a smartphone. This meets the travel safety need while removing the risks associated with internet access, social media, and AI-driven apps.

8.4 Breach of Policy and Confiscation

Any pupil found in possession of a mobile device during the school day will be subject to the school's Behaviour Policy:

- **Immediate Confiscation:** The device will be confiscated and stored in the school safe.
- **Parental Collection:** Confiscated devices will only be returned directly to a parent or carer, not to the pupil.

- **Search Powers:** Under the **Education and Inspections Act 2006**, staff have the power to search a pupil's bag or locker if they have reasonable grounds to suspect a prohibited item (including a hidden phone) is present.
- **Examination of Content:** If there is a "good reason" to suspect the device contains harmful or illegal material (e.g., deepfakes or evidence of cyber-bullying), the **DSL (Sue Hayward)** will be informed, and the device may be examined in line with the procedures in Section 6.3.

9. Staff Using Work Devices Outside School

9.1 Technical Security and MFA

Staff provided with a school laptop, tablet, or mobile device must adhere to the following security protocols to protect the school's network and pupil data:

- **Multi-Factor Authentication (MFA):** MFA must be enabled on all work devices. Staff must not attempt to bypass or disable MFA prompts when accessing school systems (e.g., MIS, email, or cloud storage) from home.
- **Central Management:** All work devices are equipped with **Mobile Device Management (MDM)** software. This allows the school to remotely lock or wipe the device if it is lost or stolen. Staff must not attempt to remove or interfere with this software.
- **Automatic Updates:** Devices must be left on or restarted regularly to allow for critical security patches and anti-malware updates. Staff should report any "update failed" notifications to the ICT Manager immediately.

9.2 Data Protection and Encryption

- **Encryption:** All portable work devices are encrypted. Staff must not save sensitive school data to any unencrypted local storage or personal cloud accounts (e.g., personal iCloud, Dropbox, or OneDrive).
- **USB and External Storage:** The use of personal USB sticks is prohibited. Any school-issued USB devices must be hardware-encrypted and password-protected.
- **Prompts and Data Entry:** When using school devices at home, staff must ensure that **Generative AI tools** are only used via school-approved platforms. No sensitive or personally identifiable pupil data should ever be entered into a public AI prompt.

9.3 Professional Boundaries and Use

- **Sole Use:** Work devices are issued for the **sole use of the staff member**. Under no circumstances should family members (including children) or friends be allowed to use a school-owned device.
- **Educational Purpose:** The device should be used only for work-related activities. Accessing high-risk sites (e.g., gambling, adult content, or unauthorized file-sharing sites) even outside of school hours is a violation of the Acceptable Use Policy and may lead to disciplinary action.
- **Physical Security:** Devices should never be left unattended in public places or visible in a car. If a device is stolen, it must be reported to the ICT Manager and the **Data Protection Officer (DPO)** within 2 hours to facilitate a remote wipe and an ICO risk assessment.

10. How the school will respond to issues of misuse

10.1 Pupil Misuse

Where a pupil misuses the school's ICT systems, internet, or AI tools, we will follow the procedures set out in our **Behaviour Policy** and **ICT Acceptable Use Policy**.

- **Proportionate Response:** Action will range from verbal reminders and loss of ICT privileges to formal suspension for serious breaches (e.g., cyber-bullying or creating deepfake content).
- **Mandatory Reporting:** Any incident involving **"Priority Harms"** (such as intimate image abuse, encouraging self-harm, or illegal AI-generated content) will be escalated immediately to the **DSL/Deputy DSL** and, where necessary, reported to the police or **CEOP**.

- **Supportive Follow-up:** Following any misuse, the school will provide educational support to help the pupil understand the digital consequences of their actions and build future resilience.

10.2 Staff Misuse

Misuse of school systems, work devices, or personal devices by staff that constitutes misconduct will be dealt with in accordance with the **Staff Code of Conduct** and **Disciplinary Procedures**.

- **Professional Boundaries:** Staff are expected to maintain clear boundaries. Misuse includes unauthorized contact with pupils via personal social media or messaging apps (e.g., WhatsApp).
- **AI Ethics:** Staff must not use non-approved AI tools to process pupil data or generate content that brings the school into disrepute.
- **Safer Recruitment:** In line with current standards, any evidence of digital misuse may be recorded and considered during future safeguarding audits or reference requests.

10.3 Cyber Incidents and Data Breaches

In the event of a technical misuse that results in a cyber-attack or data breach (e.g., ransomware or unauthorized data access):

- **Internal Reporting:** The incident must be reported immediately to the **ICT Manager** and **DPO**.
- **External Reporting:** The school must report "serious cyber-attacks" to the **DfE Cyber Incident Support Team** and, if personal data is compromised, to the **Information Commission** within 72 hours.
- **Containment:** The school will follow its **Cyber Incident Response Plan** to isolate affected systems and protect the wider network.

10.4 Illegal Activity

The school will always cooperate with external agencies. We will report to the police any activity that involves:

- Indecent images of children (including AI-generated content).
- Threats of violence or extreme harassment.
- Accessing or distributing terrorist or extremist material.
- Serious financial fraud or "hacking" offences under the **Computer Misuse Act**.

11. Training

11.1 Staff Induction and Annual Training

All staff, including temporary and supply staff, will receive a robust safeguarding induction. This training explicitly includes:

- **The "Four Cs" of Online Risk:** Understanding Content, Contact, Conduct, and **Commerce** (specifically online scams and gaming "loot boxes").
- **AI Literacy:** Recognising the risks of **deepfakes** (both image and audio) and the ethical use of Generative AI in the classroom.
- **Filtering and Monitoring Responsibilities:** Understanding their role in the school's technical defence—specifically what to do if they see a "Red Flag" alert or suspect a child is bypassing filters.
- **Cyber-Hygiene:** Mandatory training on identifying sophisticated AI-generated phishing attacks and the proper use of **Multi-Factor Authentication (MFA)**.

Refresher Frequency: All staff will receive a formal safeguarding update at least annually. "Bite-sized" updates (e.g., via the weekly staff briefing or "Safeguarding Spotlight" emails) will occur at least half-termly to keep pace with rapid tech changes.

11.2 The Designated Safeguarding Lead (DSL)

The DSL and any deputies will:

- **Level 3 Training:** Undertake advanced safeguarding training at least **every 2 years**.
- **Annual Knowledge Updates:** In line with current standards, the **DSL** must update their skills on online safety **at least annually**. This includes attending specific briefings on **AI-generated harm** and **digital radicalisation** (Prevent Duty).
- **Technical Oversight:** The DSL will receive specific training on how to interpret and act upon the school's **filtering and monitoring logs**.

11.3 Governors and Volunteers

- **Strategic Oversight:** Governors will receive training that equips them to "strategically challenge" the school's online safety provision. This includes knowing how to audit the **filtering/monitoring logs** and ensuring the school meets the **DfE Digital Standards**.
- **Volunteers:** All regular volunteers will receive an online safety briefing as part of their induction, focusing on professional boundaries and the "No Private Messaging" rule.

12. Monitoring and Review

Logging and Incident Management

The DSL maintains a central, secure log (CPOMS) of all online safety incidents. This includes:

- **Low-Level Concerns:** "Near-misses" or minor AUP breaches that may indicate a developing trend.
- **Filtering Alerts:** Any "Red Flag" events generated by the school's monitoring software.
- **Action & Outcome:** Clear documentation of the support provided to the pupil and any communication with parents or external agencies.