ETTINGTON C of E PRIMARY SCHOOL

AND PRE-SCHOOL

Reviewed September 2026

Ettington Church of England
Primary School

Learning for Fullness of Life
Trust- Respect - Love

ONLINE SAFETY POLICY

---

1. INTRODUCTION AND POLICY AIMS

This Online Safety Policy has been updated to reflect the rapidly evolving digital landscape and to align with the latest statutory guidance - Keeping Children Safe in Education (KCSIE, 2026). It is designed to be read in conjunction with our suite of safeguarding policies and GDPR policies.

We aim to create experiences that make our children feel safe, valued, and inspired, ensuring everything we do enhances the life it touches. This policy is a core component of this strategy, extending our commitment to "unreasonable hospitality" to the digital world. We believe that true flourishing encompasses holistic growth, including social and emotional well-being.

This policy aims to:
● Promote a whole-school approach to online safety, recognising it as an integral part of safeguarding.
● Set clear expectations for the online behaviour, attitudes, and activities of all members of Ettington Primary School, especially staff, when using digital technology.
● Help staff recognise and respond to online safety risks and build resilience, both for themselves and for the children in their care.
● Facilitate the safe, responsible, respectful, and positive use of technology to support teaching and learning.
● Establish clear structures for treating online misdemeanours and procedures to follow when concerns arise, linking with our Behaviour Policy and Anti-Bullying Policy.

2. KEY PEOPLE

This policy is a living document, subject to full annual review and amendment as necessary in response to developments within Ettington Primary School and Pre-School, the local area and national guidance.

Key Personnel for Online Safety:
● Designated Safeguarding Lead (DSL), with lead responsibility for online safety, including filtering and monitoring: Michelle Crowe (Headteacher)
● DSLs and Deputy Designated Safeguarding Leads (DDSLs): Sherrel Brown (Deputy Head Teacher, DSL, SENCO)
● Link Governor for Safeguarding: Heather Fletcher (Chair of Governors)
● Network Manager / Technical Support: (Managed by Warwickshire ICT Development Service)

3. SCOPE OF THE POLICY

This policy applies to all members of the Ettington community, including teaching staff, teaching assistants, supply staff, support staff, governors, volunteers, contractors, pupils, parents/carers, and visitors. It covers all access to and use of school digital systems, both on and off-site, and the use of personal digital technology on school premises (where allowed). The Headteacher is empowered to regulate the behaviour of pupils when they are off the school site and to impose disciplinary penalties for inappropriate behaviour that is linked to membership of the school, including online bullying and other online safety incidents.

4. CURRENT ONLINE SAFEGUARDING TRENDS AND RISKS

Technology and the associated risks and harms evolve rapidly. Ettington Primary School and Pre-School conducts an annual review of its approach to online safety, supported by an annual risk assessment that considers the risks our children face.

Nationally, recent trends include:

● **Rapid rise of Generative AI (GenAI):** Thousands of sites offer AI-generated content, including abusive, pornographic, and illegal material. Platforms hosting AI "girlfriends," unregulated therapy bots, and chatbots encouraging self-harm or suicide are accessible to students. AI-generated child sexual abuse material (CSAM) is illegal to create, possess, or share.
● **High screen time:** Children aged 8-14 spend an average of 2 hours 59 minutes a day online across various devices.
● **Underage social media use:** Over half of 3-12-year-olds use at least one social media app, despite minimum age requirements (typically 13+). Four in ten admit to giving a fake age online, exposing them to inappropriate content and increasing harm.
● **Self-generated sexual content:** The Internet Watch Foundation (IWF) Annual Report noted an increase in 3-6-year-olds tricked into self-generated sexual content and more 7-10-year-olds visible in CSAM images than 11-13s. For secondaries, 217,780 cases of self-generated CSAM were found for 11-13-year-olds, predominantly girls. There's also an increasing risk of financial sexual extortion ('sextortion') among older teenage boys.
● **Social media as a news source:** Growing numbers of children and young people use platforms like TikTok for news, often with little attention to facts or veracity.
● **Filming interactions:** Safeguarding concerns arise when parents film interactions with staff outside school gates and post on social media.
● **Cyber Security:** The education sector remains a target for cyber-attacks, with 60% of secondary schools and 44% of primary schools reporting a breach or attack in the past year.

Ettington Primary School and Pre-School has a duty to ensure staff and children understand these evolving issues and the vocabulary associated with online safety. These risks can be categorised into four areas, known as the 4 Cs:

● **Content:** Exposure to illegal or harmful material, now explicitly including antisemitism, disinformation (including fake news), and misinformation.
● **Contact:** Harmful online interaction, specifically including being subjected to interaction with generative AI applications that simulate human interaction (e.g., AI chatbots).
● **Conduct:** Online behaviour that causes harm, including making, sending, or receiving explicit images generated using AI.

● **Commerce:** Risks such as online gambling, phishing, or financial scams.

5. ROLES AND RESPONSIBILITIES FOR STAFF

All staff members are crucial to maintaining a safe online environment and fostering a culture of safeguarding. In line with our Staff Behaviour Policy (Code of Conduct), unacceptable behaviour such as discrimination, bullying, harassment, or intimidation will not be tolerated.

All Teachers and Teaching Assistants must:

● Read, understand, and adhere to Ettington Primary School and Pre-School Staff Acceptable Use Policy (AUP), Safeguarding and Child Protection Policy, Staff Behaviour Policy (Code of Conduct), Mobile Phone Policy, Smartwatch and Wearables Policy, and Whistleblowing Policy.

● Familiarise themselves annually with KCSIE.

● Complete mandatory online safety and child protection training at induction and receive regular updates (at least annually).

● Maintain an awareness of current online safety issues and trends, including those related to AI, and understand that online safety is a core part of safeguarding.

● Know the identity of the Designated Safeguarding Lead (DSL) and Deputy DSLs (DDSLs) in their school and how to contact them.

● Immediately report any suspected misuse or problem to the DSL (or a DDSL) for investigation and action, no matter how small it may seem. This includes concerns identified through filtering and monitoring systems.

● Ensure all digital communications with pupils and parents/carers are professional and only carried out using official school systems and devices. Personal email addresses, text messaging, or social media must not be used for these communications.

● Model safe, responsible, and professional online behaviours in their own use of technology, both within and outside school, and in their use of social media.

● Supervise and monitor the use of digital technologies, mobile devices, and cameras in lessons and other school activities, implementing current policies.

● Ensure pupils understand and follow the Online Safety Policy and Acceptable Use Policies.

● Help pupils develop critical thinking skills to validate information, avoid plagiarism, and uphold copyright regulations when accessing online materials.

● Understand the benefits and risks of Artificial Intelligence (AI) services in school and be transparent in their use, prioritising human oversight. AI should assist, not replace, human decision-making, and all AI-generated content must be fact-checked and critically evaluated before sharing or publishing.

● Avoid entering child data or sensitive information into generative AI systems.

● Adhere to the ICTDS technical security policy regarding devices, systems, and passwords, and have a basic understanding of cybersecurity.

● Understand how children in their care use digital technologies out of school to be aware of potential online safety issues.

● Contribute to the development of safeguarding policy and practice.

6. EDUCATION AND CURRICULUM

The education of pupils in Online Safety/Digital Literacy is an essential part of our school provision. We believe in the power of technology but also in the power of decent human beings, teaching children to be ethical and responsible citizens.

Our Online Safety Education Programme:

● A planned Online Safety curriculum is provided as part of Computing and PSHE/RSHE lessons, and reinforced across all curriculum areas.

● Key Online Safety messages are reinforced through assemblies, pastoral activities, and other initiatives like Safer Internet Day and Anti-Bullying (Positive Noticing) Week.

● Pupils are taught to be critically aware of online materials, validate information, acknowledge sources, and respect copyright.

● Resilience to radicalisation is built by providing a safe environment for debating controversial issues and promoting understanding of influence and participation in decision-making.

● The curriculum promotes healthy and respectful online relationships, the effects of online actions on others, and how to recognise and display respectful behaviour.

● Learning about Artificial Intelligence (AI) is integrated, supporting learners to understand how GenAI works, its benefits, risks, and ethical and social impacts. This prepares pupils to harness the potential of new technologies like AI responsibly.

. ● We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will access.

7. HANDLING SAFEGUARDING CONCERNS AND INCIDENTS

Online safety is an integral part of safeguarding; therefore, concerns must be handled in the same way as any other safeguarding concern. All staff are expected to maintain an attitude of 'it could happen here' where safeguarding is concerned and to act in the best interests of the child.

Reporting Procedures:

● Any suspected online risk or infringement must be reported to the Designated Safeguarding Lead (DSL) or a Deputy DSL as soon as possible on the same day.

● All concerns must be recorded on CPOMS.

● If in exceptional circumstances the DSL or Deputy DSL is unavailable, staff should speak to a member of the senior leadership team and/or seek advice from local authority children's social care (Family Connect). Any action taken must be shared with the DSL/Deputy DSL as soon as possible.

● Data Protection Act 2018 (DPA) and UK GDPR do not prevent the sharing of information for safeguarding purposes. Fears about sharing information must not stand in the way of safeguarding children.

● Low-level concerns (behaviour towards a child that does not meet the harms threshold but causes unease) about staff must be reported to the Headteacher. If the concern is about the Headteacher, it must be reported to the Chair of Governors. These are then referred to the Local Authority Designated Officer (LADO) if the concern meets the threshold.

● Whistleblowing procedures are in place for staff to raise concerns about poor or unsafe practice or potential failures in safeguarding provision. The NSPCC Whistleblowing Advice Line (0800 028 0285) is an alternative route.

● If there is any suspicion of illegal activity (e.g., child abuse images), staff must report immediately to the police.

● The school will inform parents/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour considered particularly concerning or breaking the law.

● The school will actively seek support from other agencies as needed (e.g., local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police and Harmful Sexual Behaviour Support Service).

● When a child leaves the school, the DSL will ensure the child protection file is transferred to the new setting within 5 days for an in-year transfer or within the first 5 days of a new term.

8. KEY ONLINE SAFETY PRIORITY AREAS

Ettington C of E Primary School and Pre-School implements specific policies and procedures to address various online safety risks:

Nudes – Sharing Nudes and Semi-Nudes

All staff must refer to the UK Council for Internet Safety (UKCIS) guidance on 'Sharing nudes and semi-nudes: advice for education settings'. Staff, other than the DSL, must NOT attempt to view, share, or delete images, or ask anyone else to do so, but must go straight to the DSL. The DSL will follow guidelines for decision-making regarding referrals.

The definition of "making or sharing nudes and semi-nudes" now explicitly includes content that has been digitally altered or wholly generated using artificial intelligence, such as "deepfakes" or "deep nudes". Staff must treat any report of AI-generated nudes as a criminal and safeguarding matter, regardless of whether the content features a real person or is entirely synthetic.

Online Bullying

Online bullying (or cyberbullying) should be treated like any other form of bullying, and the school's Anti-Bullying Policy must be followed. This includes issues arising from "banter". Staff are reminded that fights are sometimes filmed or live-streamed, and fake profiles are used to bully children.

Child-on-Child Sexual Violence and Sexual Harassment

Ettington Primary School and Pre-School adopts a zero-tolerance approach to all forms of child-on-child abuse, including sexual violence and sexual harassment, both online and offline. Staff must not dismiss incidents as “banter” or “part of growing up”. All staff receive training on harmful sexual behaviour (HSB). Incidents are reported to the DSL, who follows KCSIE Part 5 guidance and works with local partner agencies to access specialist support for victims and alleged perpetrators. The DSL regularly analyses reports to identify and respond to emerging trends.

Extremism and Radicalisation (The Prevent Duty)

Ettington Primary School and Pre-School has a statutory duty under the Prevent Duty to prevent people from being drawn into terrorism. This duty is part of our wider safeguarding obligations. School assess local risks, works in partnership with police and local Prevent Officers, and all staff complete Prevent training (annually). DSLs also complete training on the Channel process. Our ICT policies include appropriate filtering and monitoring to protect children online.

Data Protection and Cyber Security

All staff are bound by the school’s Data Protection Policy. We comply with the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR), ensuring personal information is processed fairly and lawfully, and kept safe and secure. Data protection does not prevent the sharing of information for safeguarding. The education sector remains a target for cyber-attacks. We are directly responsible for having appropriate security protection procedures and reviewing their effectiveness. Staff receive training on cyber threats and data security awareness.

Technical Infrastructure and Network Security

Ettington Primary School and Pre-School is responsible for ensuring that the school network is as safe and secure as is reasonably possible, and that approved policies and procedures are implemented. Our IT system security is a managed service, insured and regularly checked, with patches and other security essential updates applied promptly by Warwickshire ICT Development Service (ICTDS) to protect personal data and systems. Administrative systems are securely ring-fenced from those accessible to learners.

Specific policies are in place to regulate various aspects of technical use and access:

● Temporary Access: An agreed policy governs temporary access for "guests," such as trainee teachers, supply teachers, and authorised visitors, onto school systems. Guest users are provided with appropriate access based on an identified risk profile.

● Personal Use of School Devices: An agreed policy defines the extent of personal use allowed on school devices, including those used outside school hours.

● Software Installation: Staff are not permitted to install software on school-owned devices without the consent of the Senior Leadership Team (SLT) or the IT service provider.

● Removable Media: The use of removable media (e.g., memory sticks) by users on school devices is not permitted.

● Email Security: The official WeLearn365 email service is regarded as safe and secure and is monitored. Users are aware that email communications are monitored, and staff and pupils must use only the WeLearn365 email service for school-related communications. Staff must

immediately report any uncomfortable, offensive, discriminatory, threatening, or bullying communications received.

● Password Management: Learners are encouraged to set passwords with increasing complexity, and users are required to change passwords if compromised. As recommended by the National Cyber Security Centre, staff must have a strong password of two or three random words, capital letter, a number and a symbol.

Appropriate Filtering and Monitoring

The DSL has lead responsibility for filtering and monitoring and works closely with technical colleagues from Warwickshire ICT Development Service to implement the DfE Filtering and Monitoring Standards.

● Clear Roles and Responsibilities for managing these systems are identified and assigned.

● Filtering and monitoring provision is reviewed at least annually, or more regularly in light of significant technological developments or incidents. The review involves the DSL, IT service provider and the responsible governor.

● Smoothwall is in place to block harmful and inappropriate content (including illegal, inappropriate, or harmful content like pornography, racism, misogyny, self-harm, radicalisation, extremism, misinformation, disinformation, and conspiracy theories) without unreasonably impacting teaching and learning. We ensure that "over blocking" does not lead to unreasonable restrictions on online safety education. Our systems aim to handle multilingual content, common misspellings, and identify/block techniques like VPNs used to bypass filters.

● Effective monitoring strategies are in place to meet safeguarding needs, with urgent alerts picked up and acted on, and outcomes recorded by the DSL. Monitoring can include device management software, in-person classroom monitoring, and network monitoring using log files.

● All staff are aware of filtering and monitoring systems and play their part in feeding back concerns, potential bypasses, or over-blocking.

● Monitoring applies to devices accessing the school network.

● Safe Search is enforced on accessible search engines on all school-managed devices, and we recommend the use of https://www.kiddle.co.

● YouTube is blocked on all pupil devices and only accessible on staff devices.

● All pupil and staff laptops are managed by ICTDS.

Use of Generative Artificial Intelligence (AI)

Our policy on GenAI includes:

● We acknowledge the potential benefits of AI to enhance learning, teaching, and administrative processes.

● We will educate pupils, staff, and parents about the practical, ethical pros and cons of AI.

● Plagiarism and cheating using GenAI are prohibited, and the Behaviour Policy will be applied for any pupil found doing so.

● Staff are not allowed to enter child data or sensitive school-related information into GenAI systems due to data risks.

● Only AI technologies approved by the school may be used, and staff must use school-provided AI accounts for work purposes.

● Human oversight is paramount; staff must critically evaluate AI-generated outputs for accuracy, bias, and discrimination before sharing or publishing. Final judgments, particularly those affecting people, must be made by humans.

● We comply with all relevant legislation and guidance, including KCSIE and UK GDPR, regarding AI.

● We will provide relevant training for staff and governors on the advantages, use, and potential risks of AI.

9. DIGITAL TECHNOLOGIES AND DEVICE USAGE

Ettington Primary School and Pre-School has clear guidelines for personal digital devices. Our intention is to create a learning environment free from unnecessary digital distractions, encouraging real-world interaction, focus, and play.

Personal Digital Devices (including Mobile Phones, Laptops, Tablets, and Wearable Devices)

● Pupils are not permitted to bring personal mobile phones, laptops, tablets, or other personal electronic devices to school for general use. Our schools operate on a "device-free" principle for pupils' personal devices during school hours to foster a focused learning environment and promote social interaction.

● Staff are not permitted to use personal laptops on school premises for work purposes. Schools are "data controllers" under UK law (GDPR) and are legally responsible for protecting the personal data of pupils and staff. Using school-provided devices, which are managed and secured by ICTDS, is the most effective way to ensure this. It prevents sensitive information from being stored on a device the school cannot control. Security and Control: School-owned devices are configured and managed with specific security measures, such as firewalls, antivirus software, and content filters. This is crucial for protecting the school's network from malware and for ensuring that staff are not accessing inappropriate material, even unintentionally. It also allows the school to monitor device usage to ensure it aligns with acceptable use policies.

● Staff will limit personal mobile phone and wearable device use to times when children are not present.

● Staff members' personal phones will remain in their bags, cupboards, or out of sight during contact time with children.

● Staff will not take pictures or recordings of pupils on their personal phones or cameras. If this is required for school activities, school-owned equipment must be used.

● If necessary, Year 6 children may bring a phone to school if they walk alone to and from the site. If this is the case, brick phones are strongly recommended. In all cases, they must be switched off on entering the site, handed to the school office for safe storage for the duration of the school day and not switched on until children are off the school site.

● In line with DfE guidance Searching, screening and confiscation: advice for schools, the Headteachers and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example, as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but exclusive to sexual images, pornography, violence or bullying.

● Important messages to/from parents can only be made via the school office and Google Classroom.

● Other personal recording devices such as smart glasses are not permitted without written permission. It is forbidden to take secret photos, videos, or recordings of teachers or children with any device.

● Volunteers, contractors, and governors must leave phones turned off in their pockets and not use them in the presence of children or to take photos/videos.

● Staff using their personal mobile phone in an emergency such as on a school trip will ensure that the number is hidden to avoid parents accessing their private phone number.

● Our approach to mobile phones is aligned with DfE guidance, which notes that many children have unlimited internet access via mobile networks, leading to risks like online harassment, bullying, and sharing of indecent images.

Digital Images and Video

The development of digital imaging has significant benefits for learning and communication, but also presents risks related to misuse, manipulation, and privacy. At Ettington C of E Primary School and Pre-School, we are committed to using digital images responsibly and transparently.

Policy for Images and Videos:

● Making and using images of pupils requires age-appropriate consent from their parents/carers.

● Consent from parents/carers will be obtained before photographs of pupils are published. This consent will specify the purposes and platforms for publication, which will include:

○ Internal: school displays.

○ School communication: school website, newsletters, prospectus

○ Official school social media accounts.

○ Official school photographs.

○ External: local publications, newspapers.

● A central GDPR log will be kept for staff to check before any photograph is published, ensuring adherence to parental consent preferences. Whenever a photo or video is taken or intended for use, the member of staff responsible will consult this log to confirm appropriate consent.

● Publicly publishing images of individual children is not permitted.

● Images for publicising the school should avoid naming the child. Photo file names/tags should not include full names.

● Images must be securely stored and used only by authorised personnel.

● Staff and volunteers may take digital/video images to support educational aims, but must follow policies on sharing, distribution, and publication, and only use authorised equipment.

● Pupils must not take, use, share, publish, or distribute images of others without their permission.

● In general, parents/carers are welcome to take videos and digital images of their own children at school events for personal use, but these should not be published or made publicly available on social networking sites, nor should they comment on activities involving other pupils.

● Pupils are taught about online reputation, digital footprint, and how images can be manipulated.

Social Media

Social media is a fact of modern life, but presents risks to professional standards, reputation, and safeguarding.

Policy for Social Media Use:

● All staff must use social media in a positive and respectful manner.

● Staff must not make any posts that are or could be construed as bullying, aggressive, rude, insulting, illegal, or otherwise inappropriate, or that might bring the school or teaching profession into disrepute. This applies to both public and private posts.

● No reference should be made on social media to pupils, parents/carers, or school staff.

● Staff should not engage in online discussion on personal matters relating to members of the school community.

● Personal opinions should not be attributed to the school or local authority.

● Security settings on personal social media profiles must be regularly checked to minimise the risk of loss of personal information.

● Staff should decline 'friend' requests from pupils and their parents and maintain a strictly professional working relationship.

● Personal contact details (email, phone, web-based identities) should not be given to pupils or parents/carers.

● Parents with concerns are urged to contact the school directly and privately, following the school's complaints procedure.

● Email / Teacher2Parents and Google Classroom or Tapestry (Reception) are the official electronic communication channels between parents and the school.

● Social media, including chat apps like WhatsApp, are not appropriate for school use for staff-parent/pupil communication or for staff-staff communication about school-related work.

● The serious consequences of inappropriate social media behaviour are highlighted by Prohibition Orders issued by the Teacher Regulation Agency for misuse.

● We advocate for the norms of "no social media before 16" and "no smartphones before high school" to support a healthier, play-based childhood. We encourage parents to respect age ratings on social media platforms.

10. CONCLUSION AND COMMITMENT

Ettington C of E Primary School and Pre-School is committed to providing a happy and nurturing environment where children feel safe, valued, and inspired. Our aim is that every member of our school community feels a sense of belonging, safety, value, and inspiration. This Online Safety Policy is a vital part of achieving this vision, safeguarding our community in the ever-evolving digital world.

We will continue to review and adapt our policies, processes, and curriculum to protect all of our children, embracing new technologies responsibly while fostering essential human skills and promoting well-being - advancing education for the public benefit and enabling everyone to flourish.