



Athelstan Online Safety Policy

School Name: Athelstan Primary School

Date of Policy: September 2026

Review Cycle: Annual

DSL / Online Safety Lead: Lisa Watson / Tommy Bentley

Nominated Governor: Jenny Buttery

Policy Statement & Vision

At **Athelstan Primary**, we believe technology is an integral part of learning and life. We aim to equip pupils with the knowledge, skills, and resilience to navigate the digital world safely. This policy forms part of our wider safeguarding framework and complies with statutory guidance including *Keeping Children Safe in Education*, *Working Together to Safeguard Children*, and *Searching, Screening and Confiscation*.

Key Roles & Responsibilities

- **Governing Body:** Holds overall accountability for ensuring online safety measures are implemented. Conducts an annual review of the school's filtering and monitoring systems alongside the Designated Safeguarding Lead (DSL) and IT lead.
- **Headteacher & Senior Leadership Team (SLT):** Ensures the policy is applied consistently across the school, allocates resources for staff training, and oversees severe safeguarding incidents.
- **Designated Safeguarding Lead (DSL):** Takes day-to-day responsibility for online safety concerns, manages safeguarding logs (CPOMS), liaises with external agencies, and ensures filtering alerts are acted upon immediately.
- **IT Technical Staff / Provider:** Ensures technical infrastructure, networks, and school-owned devices meet standards set out by the Department for Education (DfE). Ensures effective filtering and monitoring setups without unduly restricting access to educational materials.
- **All Staff:** Read, understand, and sign the Staff Acceptable Use Policy (AUP) annually. Model safe online practices, teach digital citizenship, and report all concerns immediately to the DSL.
- **Pupils:** Follow the child-friendly Acceptable Use Rules and report any content, contact, or behavior that makes them feel uncomfortable.

Managing Risk: The 4 Cs

Our curriculum, technical controls, and reporting procedures address the four key areas of online risk:

Risk Category	Definition	School Strategy
Content	Exposure to illegal, inappropriate, or harmful material (e.g., violence, misogyny, hate speech, age-restricted material, misinformation).	Managed via age-appropriate web filtering, monitored access, and critical-thinking instruction within Computing and RSHE.
Contact	Interaction with unknown adults or peers (e.g., grooming via online games, commercial exploitation, messaging apps).	Restricted communications on school devices; explicit teaching on online communication boundaries and privacy settings.
Conduct	Personal behavior that causes harm (e.g., online bullying, unkindness in group chats, unauthorized photo sharing).	Enforced via the School Behavior Policy, clear boundaries on personal devices, and lessons on empathy and digital footprints.
Commerce	Financial exploitation, scams, hidden costs, or illicit trading (e.g., in-app purchases, loot boxes in games like <i>Roblox</i>).	School devices block app stores/purchases; guidance provided to parents regarding home settings and game mechanics.

Technical Infrastructure, Filtering & Monitoring

- Filtering & Monitoring:** The school uses an appropriate filtering system that blocks access to harmful, illegal, or inappropriate content. Monitoring software generates real-time alerts for high-risk search terms, keywords, or activity related to suicide, self-harm, radicalization, extreme violence, or indecent images.
- Annual Review:** The DSL, IT Lead, and Lead Governor formally test and review filtering and monitoring efficacy at least once per academic year.
- Generative AI & Synthetic Media:**
 - The school recognises risks associated with AI, including synthetic images, altered audio, and automated content generation.

- Pupils are taught to verify AI-generated output critically.
- Any creation, distribution, or viewing of non-consensual synthetic images or sexually explicit AI media is treated as a major safeguarding concern and handled under child protection protocols.

Mobile Phones & Personal Smart Devices

- **Pupils:** Athelstan Primary is a mobile phone-free environment for pupils.
 - Pupils are not permitted to use mobile phones, smartwatches with cellular/camera capabilities, or personal electronic devices during the school day.
 - If a pupil brings a phone to school for travel safety, it must be switched off and handed to the class teacher at registration (or Breakfast Club staff if they are attending) and collected at home time.
- **Staff:** Staff may only use personal mobile phones or cameras during non-contact times. Personal devices must **never** be used to photograph, record, or contact pupils.
- **Visitors & Volunteers:** Must keep personal devices out of sight while on school premises.

Reporting & Responding to Incidents

- **Pupil Reporting:** Pupils are reminded regularly to tell a trusted adult or use emotion tokens to instigate a discussion if something online frightens, upsets, or confuses them.
- **Safeguarding Logs:** Staff must record all online safety incidents, including online bullying or inappropriate content searches, on CPOMS within 24 hours (or immediately if high risk).
- **Indecent Images of Children (including peer-on-peer/AI):** If an indecent or semi-indecent image is suspected on a device:
 1. Do **not** view, print, duplicate, or forward the image.
 2. Isolate and secure the device immediately.
 3. Inform the DSL without delay.
 4. The DSL will contact the Police / Safeguarding Hub according to local authority guidelines.

Curriculum & Education

Online safety is integrated throughout the primary curriculum:

- **EYFS / Key Stage 1:** Focuses on fundamental rules: asking an adult before going online, keeping personal information private, and identifying trusted adults.
- **Key Stage 2:** Focuses on digital footprints, recognising online scams/grooming tactics, understanding copyright/AI, managing peer pressure online, and dealing with online bullying.
- **Parents & Carers:** The school sends regular updates via newsletters, holds annual parent workshops, and distributes guidance on popular games, social platforms, and home filtering setups.

Policy Review

This policy is reviewed annually by the DSL and approved by the Governing Body. Please also refer to the school's separate AI Policy.

- **Approved by Governors:**
- **Next Review Date:** September 2027