



KNUZDEN ST OSWALD'S CHURCH OF ENGLAND PRIMARY ACADEMY

ONLINE SAFETY POLICY

MISSION STATEMENT

Encouraging God's Children with Courage, Compassion and Creativity

OUR CORE VALUES

Kindness, Politeness, Patience, Respect, and Self-Control, all firmly rooted in Agape, Love

KINDNESS/POLITENESS

To teach our children to be kind and polite to all in good times and in adversity, as one has no idea what others are going through #justbenice

PATIENCE

To develop a community where God's love and grace can be reflected upon, and a positive peace of mind and purpose in life can be found

RESPECT

To foster respect for all in our school community, and compassion for those in the local and global communities

SELF-CONTROL

To teach our children to face challenges, developing resilience and empathy, whilst fostering self-confidence and a positive approach to learning

Our Vision

Through and with our biblical quote, '*Stand firm in the faith and do everything with love*' 1 Corinthians 16.13, we aim to create a loving school and work family community where everyone is valued and can flourish. Our quote is an affirmation that we are part of God's huge plan, and that, although the road may not always be smooth, we must be strong and be courageous. We stand firm in the faith, doing the right thing, not the easy thing and we do everything with love at the core.

1. Introduction and Ethos

At Knuzden St Oswald's, we understand that the internet and related technologies are essential for effective learning and social development. However, they also present risks. Our approach is not to simply block usage, but to empower our pupils with the skills, knowledge, and resilience to navigate the digital world safely.

This policy reflects our commitment to safeguarding children and promoting **Digital Citizenship** through a structured, evidence-based curriculum.

2. Aims of the Policy

- To safeguard and protect all members of the school community online.
- To clearly define the roles and responsibilities of staff, governors, and pupils.
- To implement the **Common Sense Education** curriculum to ensure digital literacy is taught consistently.
- To support parents and carers in understanding online risks and how to manage them at home.

3. Curriculum and Delivery

The core of our online safety education is delivered using the **Common Sense Education Digital Citizenship Curriculum**. This research-backed framework addresses the complexities of the digital world in an age-appropriate manner.

Delivery Schedule

Online safety is not a one-off event. It is embedded into our school year as follows:

- **Frequency:** Dedicated Digital Citizenship lessons are delivered **once every half term** in every year group (EYFS to Year 6).
- **Integration:** In addition to these dedicated sessions, online safety principles are reinforced during Computing lessons, PSHRE, and whenever technology is used in the classroom.

Curriculum Key Areas

The Common Sense Education plans cover six core concepts which are revisited and deepened as children progress through the school:

1. **Media Balance & Wellbeing:** Finding a healthy balance between online and offline activities.
2. **Privacy & Security:** Managing passwords and protecting personal data.
3. **Digital Footprint & Identity:** Understanding that online activity leaves a permanent record.
4. **Relationships & Communication:** How to communicate kindly and handle cyberbullying.
5. **Cyberbullying, Digital Drama & Hate Speech:** Recognizing and standing up to negativity online.
6. **News & Media Literacy:** Identifying credible sources and understanding copyright.

4. Roles and Responsibilities

The Designated Safeguarding Lead (DSL)

- Holds overall responsibility for online safety safeguarding.
- Maintains a log of online safety incidents.
- Ensures that "Appropriate Filtering and Monitoring" standards are met.

The Computing Lead / Class Teachers

- **Computing Lead:** Ensures the Common Sense Education plans are up-to-date and resources are available for the half-termly delivery.
- **Teachers:** Deliver the half-termly Common Sense lessons, model good digital behavior, and report any concerns immediately via [School's Reporting System, e.g., CPOMS].

Pupils

- Follow the pupil **Acceptable Use Agreement (AUP)**.
- Participate in the half-termly online safety lessons.
- Report anything that makes them feel uncomfortable (The "Stop, Close, Tell" rule).

Parents and Carers

- Endorse the school's Acceptable Use Agreement.
- Support the school by reinforcing the lessons taught in the Common Sense curriculum at home.

5. Managing Infrastructure and Filtering

The school employs appropriate **filtering and monitoring systems via Cidari Trust level software and hardware provision** to restrict access to inappropriate content.

- **Filtering:** Blocks access to illegal or inappropriate websites (e.g., gambling, radicalisation) using Smoothwall, provided and managed by a Cidari Trust approved technical team. Alerts are generated automatically from the always-on filtering. These alerts are emailed directly to the Headteacher.
- **Monitoring:** The filtering system send email alerts directly to the Headteacher at the point of an inappropriate search or website access attempt.
- **Reporting:** Staff must report if a legitimate site is blocked or if an inappropriate site is accessible. The Headteacher can generate reports in real time based on user, device or search category.

6. The 4 C's of Online Risks

In line with *Keeping Children Safe in Education (KCSIE)*, our curriculum and vigilance focus on:

- **Content:** Being exposed to illegal, inappropriate, or harmful content (e.g., violence, fake news).
- **Contact:** Being subjected to harmful online interaction with other users (e.g., grooming, cyberbullying).
- **Conduct:** Personal online behavior that increases the likelihood of, or causes, harm (e.g., sending abusive messages).
- **Commerce:** Risks such as online gambling, inappropriate advertising, or financial scams.

7. Responding to Incidents

If an online safety incident occurs (e.g., cyberbullying, exposure to bad content):

1. **Stop:** The child is taught to stop using the device immediately.
2. **Report:** The incident is reported to the teacher or DSL.
3. **Record:** The staff member records the incident in the safeguarding log.
4. **Action:** The DSL decides on the appropriate action (parental contact, disciplinary action, or police involvement if illegal).

8. Use of Images and Video

- Written consent is obtained from parents/carers for the use of photographs or video on the school website or social media.
- Pupils' full names are never used alongside their photographs on public platforms.
- Staff must only use school-owned devices for capturing images of students.

9. Social Media and Personal Devices

- **Pupils:** Mobile phones are not permitted for use by pupils during the school day. If brought to school, they must be handed in to the school office.
- **Staff:** Personal phones should only be used in designated areas (e.g., the staff room) and not in the presence of pupils.

10. Review

This policy will be reviewed annually by the Governing Body and the Headteacher to ensure it remains up-to-date with statutory guidance and the evolving digital landscape.

Signed: _____ (Headteacher)

Signed: _____ (Chair of Governors)

Danielle Marshall – Computing Lead – September 2025