



Cheadle Catholic Junior School
"Following in the footsteps of Jesus"

Online Safety Policy

Version	Author	Policy approved by	Approval date	Review date	Changes made?
V1	R. Fender	Full Governing Body	November 2022	November 2024	
V2	R. Fender	Full Governing Body	November 2024	November 2026	Yes
V3	R. Fender	Full Governing Body	September 2026	September 2028	Yes – Changes to AI Text reduced to ensure clarity

Contents

Scope & Legal Framework	3
2. Roles & Responsibilities	4
3. Technical Infrastructure, Cyber Security & AI	5
Filtering & Monitoring.....	5
Cyber Security.....	5
Artificial Intelligence (AI) Policy	5
4. Mobile Technologies & Digital Media.....	6
Mobile Devices & BYOD.....	6
Digital Images & Media	6
5. Communications & Social Media	7
6. Incident Management & Safeguarding Protocols.....	7
Illegal Material & Immediate Risk	7
Child-on-Child Online Abuse & Nude/Semi-Nude Imagery	7
School Sanctions.....	7

Scope & Legal Framework

- This policy applies to all members of the school community—including staff, pupils, governors, volunteers, parents, and visitors—who access school digital systems or devices on or off site.
- This policy operates in accordance with the **Online Safety Act**, statutory **Keeping Children Safe in Education (KCSIE)** guidance, DfE digital standards, and the **Education and Inspections Act 2006**.
- Under the Education and Inspections Act 2006, the Headteacher and staff are empowered to regulate pupil behaviour and apply disciplinary sanctions for off-site online misconduct (including cyberbullying) that impacts members of the school community.

2. Roles & Responsibilities

Role	Core Online Safety Responsibilities
Governing Body	Approves and monitors policy effectiveness, reviews CPOMS e-safety logs, and ensures technical infrastructure prevents access to extremist material.
Headteacher & SLT	Holds overall duty of care, manages allegations against staff, ensures staff training, and oversees monitoring support structures.
DSL & Online Safety Lead	Manages day-to-day e-safety logs/incidents using Smoothwall portal, liaises with technical staff, and reports termly to Governors and SLT.
Technical Staff (hi-impact)	Secures network infrastructure, enforces password policies, manages filtering/monitoring, and maintains system logs.
Teaching & Support Staff	Sign the Acceptable Use Policy (AUP), embed online safety across the curriculum, monitor classroom tech use, and report concerns immediately.
Pupils & Parents	Follow Acceptable Use Agreements, report online abuse, and maintain safe technology practices outside of school.

3. Technical Infrastructure, Cyber Security & AI **Filtering & Monitoring**

- In alignment with DfE standards, the DSL and Online Safety Lead maintain joint oversight with technical staff (hi-impact) regarding filtering and monitoring systems.
- The school conducts documented termly testing of filtering effectiveness and maintains audit logs of blocked access attempts.
- Broadband filtering actively blocks illegal content (Internet Watch Foundation CAIC list) and extremist material.

Cyber Security

- Multi-Factor Authentication (MFA) is mandatory for all staff accessing remote systems, cloud email, or safeguarding software (CPOMS) off-site.
- Personal data stored on removable media or laptops must be encrypted and password-protected.
- Major cyber incidents or data breaches will be reported to the Headteacher and escalated to the National Cyber Security Centre (NCSC), Action Fraud, and the ICO within 72 hours where required.

Artificial Intelligence (AI) Policy

- Staff may use sandboxed generative AI tools (such as Google Gemini) via official work accounts for administrative and lesson planning tasks.
- Staff are strictly prohibited from inputting personal, sensitive, or identifiable pupil/staff data into public generative AI platforms.
- Pupils are not permitted to access or use generative AI tools on school devices or networks.
- The creation, sharing, or viewing of AI-generated synthetic imagery, deepfakes, or altered media targeting any member of the school community is strictly banned.

4. Mobile Technologies & Digital Media

Mobile Devices & BYOD

- Cheadle Catholic Junior School does not permit Bring Your Own Device (BYOD) for pupils; pupil-owned devices are not allowed in school.
- Staff and authorized visitors may bring personal mobile devices on site but cannot connect to internal school networks or wireless infrastructure without explicit SLT approval.

Digital Images & Media

- Parental consent must be obtained before publishing pupil photographs on the school website or official communications.
- Pupil images must only be taken on school-owned equipment—staff personal devices must never be used.
- Full pupil names will never be published alongside photographs.
- Parents taking photos/videos at school events may do so for personal use only and must not publish images featuring other pupils on social media.

5. Communications & Social Media

- All digital communication between staff, pupils, and parents must be professional and conducted exclusively through official, monitored school channels.
- Staff must not use personal email addresses, text messaging, or personal social media accounts to communicate with pupils or parents.
- Staff personal social media accounts must never reference pupils, parents, or school business, nor bring the school into disrepute.

6. Incident Management & Safeguarding Protocols

Illegal Material & Immediate Risk

- If child sexual abuse imagery, grooming, or violent extremism is suspected, staff must immediately halt monitoring, isolate the affected device, and notify the Headteacher/DSL.
- The school will immediately report illegal incidents to the Police and CEOP.

Child-on-Child Online Abuse & Nude/Semi-Nude Imagery

- Incidents involving nude/semi-nude image sharing or AI-generated deepfake media will be managed under UKCIS guidance (*Sharing Nude and Semi-Nude Images*) and KCSIE.
- **Mandatory Staff Protocol:** Staff must **not** copy, print, save, or forward the image. Staff must immediately isolate the electronic device, log the incident on CPOMS, and notify the DSL for risk assessment.

School Sanctions

- Inappropriate online behavior (such as cyberbullying or bypassing filters) will be managed proportionately through the school's standard **Behaviour Policy** and **Anti-Bullying Policy**.