SS John Fisher & Thomas More
Catholic Primary School
A VOLUNTARY ACADEMY

DEUS PRIMUS

Online Safety Policy

Policy written:	July 2018
Policy reviewed:	November 2025
Governor committee responsibility:	Local Governing Body

Rationale

The internet and digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for both staff and pupils. It is the entitlement of every pupil to have safe access to the internet and digital technologies to enrich and enhance learning. This policy applies to all pupils, teaching staff, support staff, governors, volunteers and contractors, and should be read alongside the School's Safeguarding and Child Protection Policy, Data Protection (UK GDPR) Policy, and Acceptable Use Policies (AUPs).

Aims

- Ensure that all pupils, including those with special educational needs and/or disabilities, use the internet and digital technologies to support, extend and enhance their learning.

- Develop pupils' understanding of the uses, importance and limitations of the internet and digital technologies, including how to avoid undesirable and harmful material and contact.

- Promote positive attitudes to online participation and collaboration, building ICT capability through independent and collaborative working.

- Ensure pupils and staff use existing and emerging technologies safely, responsibly and ethically, including AI-enabled tools.

Principles for Internet Use

- Internet use will support, extend and enhance learning with clear objectives provided for pupils.

- Web content will be subject to age-appropriate filtering and monitoring applied across the school network and devices, without unreasonably impacting teaching and learning.

- Internet use will be embedded within the curriculum, including Computing, PSHE/RSE and cross-curricular projects.

Teaching and Learning: Building Digital Literacy and Resilience

- Teach pupils to research effectively, question reliability, identify misinformation and disinformation, and evaluate online sources (including AI-generated content).

- Explicitly teach pupils how to report inappropriate or harmful content/contact and seek help, including via trusted adults and reporting tools.

- Provide regular, age-appropriate online safety education aligned to UKCIS Education for a Connected World framework across eight strands (e.g., self-image and identity, online relationships, reputation, bullying, managing information, wellbeing, privacy/security, copyright/ownership).

Safe Use of Technology

- Pupils are taught how to use technologies safely, including social media, gaming, livestreaming and messaging platforms.

- Staff model safe and professional use of technology, adhering to AUPs and staff behaviour (code of conduct) policies.

Internet Access and Acceptable Use

- Parents/carers provide consent for internet access and sign the pupil AUP on admission; pupils agree age-appropriate rules annually.

- Staff and volunteers sign the staff AUP and receive induction and annual refresher training.

• Pupils are taught to use the internet responsibly and report concerns to a responsible adult.

Mobile Phones and Personal Devices

• Staff mobile phones must be silent or switched off during teaching time and used in line with staff AUP and code of conduct.

• Pupil devices follow age-appropriate rules; any Bring Your Own Device (BYOD) arrangements are covered by risk assessment and technical controls (e.g., filtering, MDM, VPN/proxy blocking).

School Website and Published Content

• The school website is managed by SLT and ICT team. Content is overseen by the Headteacher (John Marciniak) and the Local Governing Body.

• Images and personal information are published in line with consent, safeguarding and data protection policies (UK GDPR/DPA 2018).

Security, Filtering and Monitoring

• ICT security is reviewed regularly with Schools ICT partners; updates and patches are applied promptly.

• Appropriate filtering and monitoring systems are in place across all devices and networks; provision is reviewed at least annually with roles/responsibilities defined (DSL, IT support, SLT, governors).

• Filtering balances safeguarding with educational access, prevents access to illegal content (e.g., CSAE/IIOC, terrorist material) and limits bypass via VPNs/proxies; monitoring includes reactive alerts and manual classroom strategies.

Communication of the Policy

• Online safety rules are visible in rooms where technology is used; pupils are informed that use is monitored.

• Online safety is included in the curriculum and revisited regularly; resources are signposted to parents via website, newsletter and workshops.

• Acceptable Use Policies for pupils, staff and volunteers are available on the website and reviewed annually.

Complaints, Misuse and Incident Response

• Pupil misuse is reported to staff and logged on CPOMS; incidents are escalated to DSL/SLT where appropriate and parents informed in line with safeguarding procedures.

• Staff misuse is reported to the Headteacher/DSL and handled under HR/disciplinary procedures aligned to safeguarding and data protection.

Whole-School Responsibilities for Online Safety

Headteacher

• Leads online safety across the school (may delegate day-to-day responsibility to the ICT subject leader and DSL).

• Ensures DSL/ICT leader have time, support and authority to discharge duties effectively; informs the Governing Body of online safety issues and policies.

Designated Safeguarding Lead (DSL) and Deputies

• Establish and maintain a safe ICT learning environment including a school-wide online safety programme.

• Create, adapt and implement online safety policy and procedures; maintain an incident log and ensure appropriate, consistent responses.

• Coordinate staff training, awareness and curriculum integration; liaise with local safeguarding partners and Trust policies.

Governing Body

• Supports the Headteacher/DSL in establishing policies, systems and procedures for a safe ICT environment.

• Ensures appropriate funding for online safety solutions, training and activities; promotes online safety to parents/carers.

ICT Support / Schools ICT Partners

• Provide technical infrastructure to support online safety, filtering and monitoring; respond to discovery of illegal materials or suspicion thereof on the network.

• Report network breaches to Headteacher/DSL/ICT leader; maintain professional conduct in personal technology use; keep skills current.

Teaching and Support Staff

• Contribute to online safety policy development and adhere to AUPs; take responsibility for data security and privacy.

• Model good practice using new and emerging technologies; include online safety regularly in the curriculum; escalate concerns appropriately.

Wider School Community (including volunteers and visitors)

• Adhere to AUPs; take responsibility for data security; develop awareness of online safety issues relevant to pupils.

• Know when and how to escalate concerns; maintain professional conduct in technology use; engage with training where appropriate.

Parents and Carers

• Support AUPs and discuss online safety with children; model appropriate technology use and seek support when concerned.

• Engage with school communications and workshops; use reporting mechanisms if worried about a child's online behaviour or safety.

Remote Learning and Use of AI/Emerging Technologies

• Remote education will be used only as a last resort, with safeguarding and data protection measures in place; staff follow behaviour/code of conduct online as in person.

• Use of AI tools must be risk assessed; staff supervise and teach pupils about limitations, bias and safe/ethical use; AI must not be used to process children's data beyond lawful bases and DPIA outcomes.

Data Protection, Privacy and Images

• The school complies with UK GDPR and DPA 2018; privacy notices are provided; data minimisation, security and retention controls are applied.

• EdTech suppliers are assessed for compliance (including the Children's Code where applicable); data processing agreements define roles and responsibilities.

Prevent Duty and Reducing Permissive Environments

- The school has due regard to the Prevent duty; online safety education builds resilience to extremist content and ideologies; visiting speaker and IT policies reduce exposure to radicalising influences.

References (statutory and best-practice guidance)

- Keeping Children Safe in Education (KCSIE) 2025 – Department for Education (GOV.UK).
- Working Together to Safeguard Children 2023 – Department for Education (GOV.UK).
- Filtering and Monitoring Standards – Meeting digital and technology standards (DfE).
- UKCIS: Education for a Connected World framework (2020 edition).
- Prevent Duty Guidance (2023) – Home Office.
- Teaching online safety in schools (DfE, 2023 update).
- Providing remote education: guidance for schools (DfE, 2024).
- ICO guidance: Education data; Children’s Code and edtech.