ST JOHN FISHER CATHOLIC PRIMARY SCHOOL

ONLINE SAFETY POLICY

Reviewed: October 2025
Next Review: October 2027
Approved By: Governing Body
Designated Safeguarding Lead (DSL): Lynsey Baulch
Headteacher: Laura Mc Laughlin
Online Safety Lead: Dawn Keto-Edwards
Safeguarding Governor: Esther Phillips

1. Catholic Ethos Statement
Our Mission Statement

We stand united in our mission to build a loving world of truth, justice, peace and wisdom.

St John Fisher Catholic Primary School is committed to safeguarding all children in our care. Rooted in Gospel values, we promote respect, safety, responsibility, and digital citizenship. We recognise both the benefits and risks associated with online activity and work in partnership with pupils, staff, parents and the wider community to ensure safe, responsible and respectful use of technology.

---

2. Policy Aims

This Online Safety Policy aims to ensure that:

- Children are protected from online harm both in and beyond school.
- Staff understand their safeguarding duties related to online behaviour and technology use.
- The school meets all statutory requirements, including Keeping Children Safe in Education (KCSIE), Prevent Duty, UK GDPR, and DfE Filtering & Monitoring Standards.
- Pupils develop safe, responsible and critical digital behaviours.
- Digital technology is used to enhance learning within a safe and controlled environment.

---

3. Statutory and Guidance Framework

This policy reflects:

- Keeping Children Safe in Education (2024/25)
- Teaching Online Safety in Schools (DfE)
- DfE Filtering and Monitoring Standards (2023)
- Prevent Duty Guidance
- UK GDPR and Data Protection Act 2018
- Education Act 2011
- Working Together to Safeguard Children (2023)

- Bexley Safeguarding Children Partnership procedures

This policy should be read in conjunction with:

- Child Protection & Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Acceptable Use Policies (Staff and Pupils)
- Mobile Devices Policy
- RSHE and Computing curriculum policies

---

4. Roles and Responsibilities

4.1 Governing Body

The Governing Body ensures:

- Online safety is integral to safeguarding arrangements.
- The school uses appropriate, effective filtering and monitoring systems.
- Regular reviews of online safety procedures and incidents.
- Annual approval of this policy.

4.2 Headteacher

The Headteacher is responsible for:

- Implementing this policy and ensuring staff compliance.
- Ensuring staff receive appropriate training.
- Ensuring filtering and monitoring meet statutory requirements.

4.3 Designated Safeguarding Lead (DSL)

The DSL:

- Oversees and manages all online safety concerns.
- Ensures staff are trained and aware of emerging online risks.
- Reviews filtering and monitoring logs.
- Liaises with external agencies where needed (police, CEOP, LA).

4.4 Online Safety Lead

Where appointed, the Online Safety Lead:

- Manages technical and operational aspects of online safety.
- Works with providers such as LGfL on filtering and monitoring.
- Supports staff and curriculum leads.

4.5 Staff

All staff must:

- Read and follow the Acceptable Use Policy.
- Model safe, responsible online behaviour.
- Use only school-approved communication channels.
- Report any online safety concerns immediately.
- Maintain professional conduct online.

4.6 Pupils

Pupils must:

- Follow the Pupil Acceptable Use Agreement.
- Report concerns to a trusted adult.
- Use technology respectfully and safely.

4.7 Parents and Carers

Parents and carers should:

- Promote safe online behaviour at home.
- Engage with school guidance on online safety.
- Not post images of children other than their own on social media.

---

5. Education and Curriculum

Online safety is taught through:

- Computing
- RSHE
- PHSE
- Assemblies, themed weeks and external workshops

Pupils learn about:

- Evaluating online content and spotting misinformation.
- Online relationships, privacy, healthy behaviours, and consent.
- Cyberbullying and how to report concerns.
- The risks of image sharing, AI-generated content, and exposure to inappropriate material (especially in KS2).
- Respecting copyright and intellectual property.

---

6. Filtering and Monitoring

St John Fisher uses LGfL filtering and monitoring systems that:

- Block access to harmful and inappropriate content.
- Provide age-appropriate monitoring across the school.
- Allow activity to be logged and reviewed.
- Are reviewed regularly and reported to governors annually.

Staff and pupils must report any access to inappropriate material immediately.

---

7. Use of Devices and Technology

School Devices

- All school devices are monitored and filtered.
- Devices must not store sensitive data unless encrypted and authorised.
- Unapproved software must not be installed.

Approved Learning Platforms

St John Fisher uses selected online platforms to support learning:

- Google Classroom
- Emile
- IXL
- Twinkl Phonics
- Maths.co.uk

- Languagenut

These platforms:

- Are used **only for educational purposes**.
- Must **not allow pupils to communicate with each other** (e.g., through chat, comments, or shared documents).
- Must only be accessed using school-issued usernames and passwords.
- Must be monitored by staff, who must report any concerns immediately to the DSL.

Pupil Mobile Phones

- Pupils may bring mobile phones to school **solely for travel safety**.
- Phones must be **switched off before entering the school site** and remain off until pupils have **exited the school site**.
- Phones must be stored inside book bags for the entire school day.
- At the start of the day, staff ensure pupils take out anything needed to avoid repeated access to book bags.
- Pupils must not access book bags during the day unless directly supervised.
- If a pupil is seen with a mobile phone during the school day, it will be confiscated and taken to the office.
- Only a parent or authorised adult may collect confiscated phones.

Staff Mobile Phones

- Staff mobile phones must be stored **out of sight at all times**, unless specific permission is granted by the Headteacher.
- Staff must not use personal phones in learning environments or in the presence of pupils.
- Staff must never use personal devices to contact pupils or parents unless authorised in exceptional circumstances.
- Staff must not take photos, videos or audio recordings on personal devices.
- Phones may only be used in designated staff areas and never while supervising pupils.

Remote Learning

- Only school-approved platforms may be used.
- Staff must use school email accounts for communication.
- Live or recorded lessons must follow safeguarding and professional conduct rules.

---

8. Managing Digital Communication and Social Media

Pupils:

- Must use only school-issued accounts.
- Must not share personal information.
- Must report inappropriate communication.

Staff:

- Must not communicate with pupils using personal accounts or social media.
- Must not reference school matters on personal social media.
- Must use only school-approved communication systems.

Published Content:

- Personal information about staff or pupils will not be shared publicly.
- Photos of children will not be published with names.
- Parental consent is required for images.

---

9. Responding to Online Safety Incidents

All concerns must be reported to the DSL. The school follows:

- Child Protection procedures
- Anti-Bullying Policy
- Behaviour Policy
- UKCIS guidance on sharing nudes or semi-nudes
- Prevent Duty
- CEOP/police referrals where criminal activity is suspected

Incidents are logged and monitored to identify patterns or repeat concerns.

---

10. Data Protection

The school complies with UK GDPR and the Data Protection Act 2018.
All personal data must be:

- Processed lawfully
- Accurate and up to date
- Secure
- Minimised
- Retained only as long as needed

Staff receive annual GDPR training.

---

11. Cyberbullying, Sexting and Online Harm

The school takes all forms of online harm seriously.

- Cyberbullying incidents are recorded and investigated.
- Parents are informed where appropriate.
- Sexting/self-generated images are managed using national UKCIS guidance.
- Where criminality is suspected, police advice is sought.

---

12. Working with Parents

The school:

- Provides guidance on home online safety.
- Shares resources from ThinkUKnow, CEOP, Childnet and LGfL.
- Asks parents to sign agreements for safe technology use.
- Encourages parents to model respectful digital behaviour.

---

13. Policy Review

This policy is reviewed every two years, or sooner if statutory guidance changes. Governors receive:

- Online safety incident reports
- Filtering and monitoring reviews
- Staff training updates

The policy is published on the school website.