St Mary's Blackbrook Catholic Primary School

Online Safety Policy

Approved by:	Full Governing Board
Policy Lead:	Headteacher
Last Reviewed:	January 2026
Next Review Date:	December 2026

Statement of Intent

St Mary's Blackbrook Catholic Primary School is committed to safeguarding and promoting the welfare of children. Online safety is an essential part of safeguarding and wellbeing and is integral to teaching and learning. This policy sets out how we will educate pupils to use technology safely and responsibly, protect them from online harm, and respond to online safety incidents in a timely and appropriate way.

Legal Framework

This policy has due regard to relevant legislation and statutory guidance including, but not limited to:

- Keeping Children Safe in Education, 2025
- Working Together to Safeguard Children, 2025
- Teaching Online Safety in Schools (DfE, 2023)
- The Education Act 2002 and Education and Inspections Act 2006
- The Children Act 1989 and 2004
- The Equality Act 2010
- Data Protection Act 2018 and UK GDPR
- The Prevent Duty Guidance and Counter - Terrorism and Security Act 2015
- The Kids Online Safety Act (KOSA), 2025

This policy operates in conjunction with:

- Child Protection and Safeguarding Policy
- Behaviour Policy and Anti-Bullying Policy
- RSHE Policy
- Staff Code of Conduct and Safer Working Practice
- Data Protection / GDPR Policy
- Remote Learning Policy
- Use of Mobile Phones and Personal Devices Policy
- Acceptable Use Agreements (Pupils, Staff, Parents/Carers and Visitors)

Scope

This policy applies to all members of the school community: pupils, staff (including supply staff), volunteers, governors, parents/carers, contractors and visitors. It applies to the use of school ICT systems and devices, personal devices used on site, and online behaviour outside school where it is linked to the school community or creates a safeguarding concern.

Aims

We aim to:

- Protect all pupils from online harm and promote a safe, respectful online culture.
- Teach pupils how to stay safe online and how to report concerns.
- Ensure effective filtering and monitoring systems are in place as part of safeguarding.
- Support staff to recognise and respond to online safety concerns through training and clear procedures.
- Work in partnership with parents/carers to support safe and responsible use of technology at home and in school.

Roles and Responsibilities

Governing Board

- Approve and review the Online Safety Policy annually.
- Ensure online safety is embedded within safeguarding and child protection arrangements.
- Ensure appropriate filtering and monitoring systems are in place and reviewed.
- Monitor online safety incidents and trends through safeguarding reports.

Headteacher

- Ensure this policy is implemented consistently across the school.
- Ensure staff receive appropriate online safety and safeguarding training.
- Ensure that concerns and incidents are managed effectively and, where appropriate, referred to external agencies.

Designated Safeguarding Lead (DSL)

- Lead on safeguarding incidents with an online safety element.
- Ensure recording and reporting systems are robust and understood by staff.
- Make referrals to Children's Social Care, CEOP or the Police where required.
- Oversee support plans for pupils who are vulnerable online.

Computing Lead

- Coordinate whole-school approaches to online safety education in conjunction with the DSL and Senior Leaders.
- Support staff with resources and guidance.
- Liaise with IT support and Senior Leaders regarding filtering and monitoring.

All Staff

- Model safe and responsible use of technology and maintain professional boundaries online.
- Follow the Staff Acceptable Use Agreement and Code of Conduct.
- Report any online safety concerns immediately to the DSL in line with safeguarding procedures.
- Ensure pupils are supervised appropriately when using technology.

Pupils

- Follow the Pupil Acceptable Use Agreement.
- Use technology respectfully and responsibly.
- Report anything that worries or upsets them online to a trusted adult.

Parents/Carers

- Support the school’s online safety expectations at home.
- Engage with school guidance and communications about online safety.
- Report concerns to the school promptly and work with staff to support safe behaviours.

Education: Teaching Online Safety

Online safety is taught as part of a broad and balanced curriculum, including Computing and RSHE, and reinforced through assemblies, themed events and pastoral support. Teaching will be age-appropriate and cover the four key areas recommended by the DfE: content, contact, conduct and commerce, alongside credibility and online manipulation.

Key themes include:

- Self-image and identity, privacy and security
- Online relationships and respectful communication
- Cyberbullying and reporting harmful behaviour
- Online reputation and digital footprints
- Managing online information, misinformation and scams
- Online risks: grooming, exploitation, sexting/self-generated images
- Radicalisation and extremism
- Healthy screen time and wellbeing

Filtering and Monitoring

The school will ensure appropriate filtering and monitoring systems are in place to protect pupils and staff from harmful and illegal content. Filtering and monitoring is part of safeguarding and will be reviewed regularly by leaders and governors. The school will ensure that staff understand how to respond to alerts and concerns, and that monitoring does not replace supervision or teaching.

The school uses Smoothwall filtering and monitoring software, including keyword and activity monitoring (KeyLog), to help identify potential safeguarding concerns such as self-harm, suicide ideation, bullying, sexual content, radicalisation or exploitation risks. Alerts are reviewed by trained staff in line with safeguarding procedures. Monitoring is proportionate and supports safeguarding; it does not replace supervision, professional judgement, or an open culture where pupils feel able to report concerns.

Acceptable Use

The school maintains Acceptable Use Agreements for pupils, staff, parents/carers and visitors. All users must sign and follow the relevant agreement. Breaches may result in sanctions in line with the Behaviour Policy and/or disciplinary procedures.

Use of Mobile Phones and Personal Devices

The school sets clear expectations for the use of mobile phones, smartwatches and other personal devices. Pupils may only use devices in line with school rules. Staff must not use personal devices to photograph pupils or communicate with pupils via personal accounts.

Responding to Online Safety Incidents

All online safety concerns must be reported immediately to the DSL. Examples include:

- Accessing or sharing inappropriate content
- Cyberbullying or online harassment
- Sexting / self-generated sexual imagery
- Grooming or inappropriate contact
- Radicalisation concerns
- Threats or coercion online
- Suspicious searches indicating self-harm or exploitation risk

Staff must not investigate illegal content. If there is concern about child sexual abuse material, grooming, extremism or serious threats, the device should be secured and the DSL informed immediately. The DSL will contact relevant agencies (e.g., Police, CEOP, Children's Social Care) in line with statutory guidance.

Data Protection and Security

All staff and pupils must follow the school's data protection procedures. Personal data must be handled securely, using approved systems only. Any data breach must be reported immediately to the Headteacher and Data Protection Lead.

Working with Parents and Community

The school will support parents/carers through guidance, workshops, newsletters and signposting to trusted resources such as the NSPCC, CEOP and the UK Safer Internet Centre.

Monitoring and Review

Online safety incidents and trends will be monitored by the DSL and senior leaders. This policy will be reviewed at least annually, or sooner in response to significant changes in guidance, technology or school practice.