

Rishton Methodist Primary School

Online Safety Policy 2025 - 2026



Our Christian Vision

As a Methodist school, our values lie at the heart of all we are and do. Within our caring Christian community, where all are welcome, everyone is encouraged to be the best that they can possibly be. We promote respect, compassion and resilience to prepare our children for the challenges of an ever-changing world and encourage our whole school community to 'Rise up...take courage and do it" (Ezra 10:4).

Agreed by Governing Board

Policy will be reviewed by September 2027

Created by Mr. Sean Steele

Introduction

Rishton Methodist Primary School recognises that digital technologies are an essential part of children's lives, learning, and future opportunities. With these opportunities come risks, and the school has a duty to ensure pupils are protected, educated, and empowered to navigate the online world safely and responsibly. This policy outlines our approach to safeguarding pupils online, promoting digital resilience, and ensuring staff, parents, and pupils understand their roles in maintaining a safe digital environment.

E-safety is not a standalone issue; it is embedded across safeguarding, behaviour, curriculum, pastoral care, and the wider ethos of the school. This policy should be read alongside the Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, and Acceptable Use Agreements.

Aims

The aims of this policy are to:

- Protect pupils from harmful or inappropriate online content, contact, and conduct.
- Ensure pupils develop the knowledge, skills, and attitudes needed to use technology safely, respectfully, and responsibly.
- Provide clear expectations for staff and pupils regarding the use of digital devices and online platforms.
- Establish robust systems for filtering, monitoring, reporting, and responding to online safety concerns.
- Support parents and carers in promoting safe online behaviour at home.
- Ensure compliance with statutory guidance, including Keeping Children Safe in Education (KCSIE) and the Prevent Duty.

Roles and Responsibilities

Governing Body

- Ensures the school meets its statutory safeguarding duties relating to online safety.
- Reviews and approves the E-Safety Policy annually.
- Ensures appropriate filtering and monitoring systems are in place and effective.

Headteacher

- Ensures the policy is implemented consistently and effectively.
- Ensures staff receive regular training and updates on online safety.
- Oversees responses to online safety incidents and ensures they are recorded and monitored.

E-Safety Lead / Computing Lead

- Leads the development of online safety education across the curriculum.
- Monitors the effectiveness of filtering, monitoring, and reporting systems.
- Provides guidance and support to staff, pupils, and parents.
- Liaises with external agencies, including the Local Authority and police, when necessary.

All Staff

- Model safe, responsible, and respectful use of technology.
- Supervise pupils' online activity and follow school procedures for reporting concerns.
- Teach and reinforce online safety messages across the curriculum.
- Use school-approved devices and platforms for all professional communication.

Pupils

- Follow the school's Acceptable Use Agreements.
- Use technology respectfully and responsibly.
- Report anything that makes them feel uncomfortable, unsafe, or unsure.
- Understand that online actions have offline consequences.

Parents and Carers

- Support the school's approach to online safety.
- Monitor and guide their child's use of technology at home.
- Engage with school-provided training, resources, and communication.
- Report concerns to the school promptly.

Curriculum and Teaching

Online safety is taught progressively from Early Years to Year 6, ensuring pupils build age-appropriate knowledge and skills. Teaching includes:

- Safe use of websites, apps, and online games.
- Understanding personal information, privacy, and digital footprints.
- Recognising and responding to cyberbullying.
- Managing online relationships and communication.
- Understanding online advertising, persuasive design, and commercial influence.
- Evaluating online information and identifying trustworthy sources.
- Recognising risks such as grooming, radicalisation, scams, and harmful content.
- Understanding how online platforms collect, use, and share data.

Teaching is delivered through Computing, PSHE, assemblies, themed weeks, and cross-curricular activities. Staff use high-quality resources aligned with the *Education for a Connected World* framework.

Misinformation and Disinformation

Understanding False Information

Children increasingly encounter online content that may be inaccurate, misleading, or deliberately harmful. As part of our safeguarding and digital literacy curriculum, pupils are taught to understand, question, and challenge false information.

- **Misinformation** is false or inaccurate information shared without intent to mislead.
- **Disinformation** is false information created and shared deliberately to deceive, influence, or cause harm.

Both can appear in videos, websites, games, social media, messaging platforms, and even AI-generated content. Children may encounter them without realising, making critical thinking an essential life skill.

Why This Matters in Primary Education

Even young children:

- Believe online content is automatically true.
- Struggle to distinguish fact from opinion.
- Are influenced by peers, trends, and algorithms.
- May repeat or share false information without understanding the consequences.

Teaching pupils to question what they see online helps protect them from:

- Scams and hoaxes.
- Manipulative content.
- Harmful challenges or trends.
- Extremist or radicalising material.
- Misleading health or wellbeing information.
- False narratives that can cause fear, confusion, or harm.

How the School Reduces the Risks

Rishton Methodist Primary School takes a whole-school approach to reducing the impact of misinformation and disinformation:

- **Curriculum Integration** — Digital literacy is embedded across subjects, teaching pupils how to check information, identify reliable sources, understand bias, and recognise persuasive techniques.
- **Progressive Skill Development** —
 - EYFS/KS1: "Not everything online is true", recognising trusted adults, simple fact-checking.
 - KS2: Evaluating sources, cross-checking information, recognising bias, understanding algorithms and echo chambers.
- **Supervised, Filtered Access** — Pupils use the internet in structured, supervised sessions with robust filtering and monitoring systems.
- **Discussion and Reflection** — Pupils are encouraged to ask questions, express uncertainty, and talk openly about what they see online.
- **Parent Partnership** — The school provides guidance, workshops, newsletters, and resources to help families support safe online behaviour at home.
- **Staff Training** — Staff receive training on recognising misinformation, supporting pupils, and responding to concerns.
- **Prevent Duty Alignment** — Staff are trained to recognise when misinformation or disinformation may be linked to extremist narratives or radicalisation risks.

Filtering, Monitoring, and Technical Controls

The school uses robust filtering and monitoring systems that:

- Block access to inappropriate or harmful content.

- Alert staff to concerning searches or behaviour.
- Record activity for safeguarding purposes.
- Are reviewed regularly to ensure effectiveness.

Pupils access the internet only under supervision. Staff use school-approved accounts and devices for all professional activity.

Use of Digital Devices

- Pupils use school devices responsibly and follow classroom rules.
- Personal devices are not permitted unless authorised for specific educational purposes.
- Staff use school devices and secure accounts for all communication and data handling.
- All devices must be password-protected and used in line with data protection requirements.

Online Behaviour and Conduct

The school expects all members of the community to behave respectfully online. Pupils are taught:

- To treat others kindly and respectfully.
- Not to share personal information.
- To report unkind or unsafe behaviour immediately.
- That cyberbullying is unacceptable and will be dealt with seriously.
- That online actions have real-world consequences.

Safeguarding and Responding to Incidents

All online safety concerns are treated as safeguarding matters. Staff follow the school's Safeguarding and Child Protection Policy when responding to:

- Exposure to harmful content.
- Cyberbullying or online harassment.
- Online grooming or contact from strangers.
- Sharing or receiving inappropriate images.
- Concerns relating to misinformation, disinformation, or radicalisation.
- Repeated risky online behaviour.

Incidents are recorded, monitored, and reviewed. Parents are informed where appropriate, and external agencies may be involved when necessary.

Working with Parents and Carers

The school supports families by:

- Providing guidance on safe home use of technology.
- Sharing updates on online trends, risks, and recommended resources.
- Offering workshops, information sessions, and newsletters.
- Encouraging open communication between home and school.

- Signposting parents to reputable online safety organisations.