Tottington Primary School

Online Safety Policy

We teach children to use technology safely and act quickly when they may be at risk online. This policy covers pupils, staff, volunteers and visitors using school systems, devices or accounts, including away from school. It also covers online incidents outside school that affect pupils' safety or the school community.

Who does what

- **Governors.** Approve and review the policy. Receive regular updates on incidents and how well filtering and monitoring are working.
- **Headteacher.** Oversees day-to-day implementation, approves digital tools in line with trust requirements and makes sure staff know how to respond to concerns.
- **Designated Safeguarding Lead (DSL).** Leads on safeguarding, reviews monitoring reports, responds to concerns and advises governors on how well the arrangements work.
- **Computing Lead and IT support.** The Computing Lead leads online safety teaching and supports staff and families. IT support maintains and tests filters, monitoring and security and shares reports with the DSL and senior leaders.
- **Everyone.** Follow the relevant acceptable use agreement. Staff supervise pupils' use, act on concerns and receive online safety training at induction and updates at least annually.

Teaching and working with families

We teach online safety through Computing and PSHE, including Relationships and Health Education. We adapt teaching for pupils with special educational needs and disabilities (SEND). Children learn about harmful content, unsafe contact (including grooming and AI chatbots), harmful behaviour (including bullying and fake images) and commercial risks such as scams and in-game purchases. They learn how to get help, protect private information and question what they see online.

In Early Years we keep screen use brief, adult-supported and linked to a clear learning or accessibility need. We check content in advance and follow the DfE's Early Years screen use guidance.

We share age-appropriate agreements and explain our filtering and monitoring to families. For home learning, we tell families which school-approved sites or apps to use and who their child will interact with. Families can raise online safety concerns with the school office or ask to speak to the DSL.

Filtering and monitoring

We use age-appropriate pupil filters and separate settings for staff to block harmful and illegal content and allow suitable learning resources. Monitoring helps staff spot risks and act on alerts. Staff supervise use and report problems. A senior leader authorises any temporary filter change for teaching. IT support logs the reason and end date.

Senior leaders, the DSL and IT support review provision at least once each academic year, and sooner if risks, devices, systems or AI tools change. We run and log regular checks and resulting actions, including for school-managed devices used off site. The review considers what our systems can detect or block in apps, live content and AI tools.

Reporting and responding to concerns

- Listen, reassure the child and tell the DSL or deputy immediately. Record the facts on CPOMS. Visitors and anyone without access should ask the DSL to arrange the record. Call 999 if a child is in immediate danger.
- If an incident involves a nude or semi-nude image of a child, including an AI-generated or altered image, do not view, copy, save, share or delete it, or ask a pupil to show or send it. Report it immediately and follow the DSL's instructions.
- The DSL follows the safeguarding policy, supports those involved, involves parents or carers when safe and makes referrals to children's social care or police as appropriate. Report concerns about an adult working at the school to the Headteacher, or to the Chair of Governors if they concern the Headteacher. The school follows its allegations and low-level concerns procedures.
- Report filtering failures and cyber incidents promptly to IT support and the DSL if a child may be at risk. Report any suspected personal data breach immediately to the trust's Data Protection Officer. The school uses its behaviour and anti-bullying procedures for misuse, including incidents outside school that affect pupils. It considers the child's age, needs and any reasonable adjustments.

Phones and images

Pupils must have no access to personal phones or similar devices, including messaging smartwatches, throughout the school day unless the school has agreed an individual exception, for example for a medical need or a reasonable adjustment. Parents and carers who need to reach their child during the day should contact the school office.

Staff, visitors and volunteers keep personal devices silent and stored away when pupils are present. Staff follow the safeguarding policy on personal devices, including smartwatches and trips. Staff use approved school equipment and systems for photos, videos and recordings, including in Early Years, and follow the school's rules on consent, storage and sharing.

Using artificial intelligence

Staff can use school-approved AI tools to reduce workload, for example to plan lessons, create resources or draft generic communications. Staff check the output and remain responsible for what they use or share. The Staff Acceptable Use Agreement sets out the rules on personal data, confidentiality and copyright.

Pupil use is limited to age-appropriate, school-approved tools under staff supervision. Pupils do not use public AI chatbots independently or sign up with personal accounts. Before approving a tool or a new use, school leaders check age limits, safeguarding, filtering and monitoring, and data protection with the DSL, IT support and the trust's Data Protection Officer as appropriate. They use the DfE's AI product safety standards and complete a data protection impact assessment where required.

Related policies and guidance

Read with the school's Safeguarding and Child Protection Policy, Behaviour and Anti-Bullying Policy, Staff Code of Conduct, acceptable use agreements and Prestolee Multi Academy Trust's Data Protection Policy and privacy notices.

Keeping children safe in education 2026 • Filtering and monitoring standard • Mobile phones in schools
Generative AI in education • AI product safety standards • AI and data protection in schools
EYFS statutory framework • Early years screen use • Teaching online safety in schools • Sharing nudes and semi-nudes