



THORNTON PRIMARY SCHOOL

Love • Respect • Ambition

ONLINE SAFETY POLICY

This policy applies to all members of the school community, including staff, pupils, parents/carers, governors, visitors, volunteers and community users.

Research continues to demonstrate that digital technologies provide significant benefits for teaching, learning, communication and administration. However, technology also presents safeguarding risks. Whilst it is impossible to eliminate every risk associated with technology use, an effective Online Safety Policy helps children and adults to develop the knowledge, understanding and skills needed to manage risk safely and responsibly.

Online safety is recognised as an essential part of safeguarding. Thornton Primary School is committed to creating a culture where children are empowered to use technology safely, responsibly and positively. The school recognises that safeguarding issues can occur both online and offline and that children may be vulnerable to a range of online harms including cyberbullying, child-on-child abuse, online grooming, child sexual abuse and exploitation, radicalisation, misinformation and disinformation, online scams, exposure to inappropriate content and risks associated with emerging technologies, including artificial intelligence (AI).

This Online Safety Policy forms part of the wider safeguarding framework and outlines how we will ensure that our school community is prepared to deal effectively with the challenges and opportunities presented by technology.

The policy is organised into four main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection

Vision for Online Safety

At Thornton Primary School, we use information technology to enhance learning opportunities for pupils and to support the efficient organisation and administration of the school.

Keeping all members of our school community safe while using technology is a priority. We expect staff to act as positive role models and to adhere to all agreed expectations relating to online conduct and use of technology.



Children are encouraged to develop independence, resilience and critical thinking when using technology. We believe that education is the most effective means of helping children navigate the online world safely. Online safety education is therefore embedded throughout the curriculum and reinforced through assemblies, pastoral support, PSHE and safeguarding activities.

The school recognises that technology continues to evolve rapidly. New technologies, software platforms and artificial intelligence (AI) applications may present both opportunities and risks. Any new technology introduced into school will be subject to appropriate safeguarding and risk assessment procedures before implementation.

The role of the school's Online Safety Champion

The Headteacher is the school's Online Safety Champion and Designated Safeguarding Lead (DSL).

The role includes:

- Ensuring that all Online Safety documents and Acceptable Use Agreements remain up to date.
- Monitoring implementation of the Online Safety Policy.
- Ensuring all staff understand reporting procedures for online safety concerns.
- Maintaining and reviewing online safety incident records.
- Keeping up to date with national guidance, legislation and emerging risks.
- Coordinating online safety education for pupils, staff, governors and parents/carers.
- Supporting the development of a whole-school culture of online safety.
- Working alongside the IT service provider to ensure filtering and monitoring systems remain effective.
- Ensuring filtering and monitoring arrangements are reviewed annually.
- Reporting online safety, filtering and monitoring arrangements to governors.
- Ensuring new technologies and AI tools are risk assessed before implementation.
- Monitoring trends in online safety incidents and responding appropriately.

Our Online Safety Champion is Mr David Ashcroft, Headteacher and DSL.

Security and Data Management

In our school, personal information is managed in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Staff are responsible for ensuring that all information is:

- Accurate



- Secure
- Processed lawfully, fairly and transparently
- Processed only for legitimate educational purposes
- Protected from unauthorised access
- Retained only for appropriate periods
- Shared securely and only where appropriate

School equipment must only be used for school purposes.

Staff must:

- Use approved school systems and accounts.
- Keep passwords secure and confidential.
- Use strong passwords and multi-factor authentication where available.
- Report any actual or suspected data breach immediately.
- Ensure school information is not stored on unauthorised personal devices.

Sensitive information must not be transmitted using personal email accounts or personal messaging applications.

Use of Mobile Devices

In our school we recognise that mobile technology can support educational activities and communication. However, appropriate safeguards must always be maintained.

Therefore:

- Staff must not use personal mobile phones whilst supervising pupils unless authorised by a member of SLT.
- Personal devices must never be used to store pupil information.
- Personal devices must never be used to photograph or film pupils.
- School staff must only use approved school systems when conducting school business.
- Any authorised use of personal devices must comply with school safeguarding and data protection procedures.

Further information can be found within the school's Mobile Phone Policy.

Use of Digital Media

All use of photographs, video and digital media must comply with safeguarding, data protection and professional conduct requirements.



In addition:

- Appropriate parental consent must be obtained.
- Full names will not be used alongside pupil photographs.
- Images must only be taken using approved school devices.
- Images must be stored securely.
- Staff must not upload pupil images to personal social media accounts.
- All photographs should be stored in approved school locations.
- Children must always be appropriately dressed.
- Permission from the Headteacher must be obtained before publication online.
- Any use of AI-generated images must comply with safeguarding, equality, copyright and data protection requirements.

Communication Technologies

Keeping Children Safe in Education highlights the importance of schools maintaining effective communication with parents and carers regarding online safety and helping parents understand how schools safeguard children online.

School communications should be professional, appropriate and conducted using authorised school systems.

Online communication with pupils and parents must always be transparent and capable of scrutiny by school leaders where required.

Email

In our school:

- Staff should use approved school email accounts for school business.
- Personal email accounts should not be used for sharing school information.
- Confidential information must only be shared securely.
- Any inappropriate email incident should be reported immediately to the Headteacher or DSL.

Social Networks and Social Media

In our school the following expectations apply:

- Personal social networking sites should not be accessed through school devices unless authorised.
- Staff should carefully manage privacy settings on personal accounts.
- Staff should avoid publishing information that could compromise their professional role.



- Staff must not accept friend or follower requests from current pupils.
- Staff must not communicate with pupils using personal social media accounts.
- Online behaviour that undermines professional standards or calls suitability to work with children into question may be managed under disciplinary procedures.

Artificial Intelligence (AI)

The school recognises the increasing availability and use of artificial intelligence technologies.

Where AI technologies are used:

- Appropriate risk assessments will be undertaken.
- Safeguarding, privacy and data protection requirements must be met.
- Staff remain responsible for verifying the accuracy and suitability of any AI-generated content used within school.
- Personal or sensitive information must not be entered into AI systems unless formally approved.
- Pupils will receive education regarding the safe, ethical and responsible use of AI tools.

New AI technologies will be reviewed regularly as their capabilities and associated risks continue to develop.

Dealing with Incidents

Any online safety concern should be treated as a potential safeguarding concern where appropriate.

All staff should report concerns immediately to the DSL.

Illegal content may include:

- Child sexual abuse material (CSAM)
- Terrorism-related content
- Criminally obscene material
- Content promoting serious violence
- Other material prohibited by UK law

Staff must never investigate suspected illegal material themselves.

Relevant concerns may be referred to:

- Children's Social Care
- Police
- Internet Watch Foundation
- Prevent and Channel partners



- Other safeguarding agencies as appropriate

Appropriate records will be maintained for all incidents and concerns.

Filtering and Monitoring

Thornton Primary School operates filtering and monitoring arrangements designed to safeguard pupils whilst supporting teaching and learning.

Filtering systems are intended to:

- Block illegal material.
- Block child sexual abuse content.
- Block terrorist and extremist content.
- Restrict access to inappropriate and harmful material.
- Support age-appropriate access to learning resources.
- Minimise exposure to harmful AI-generated content where technically possible.

Monitoring arrangements are intended to:

- Identify safeguarding concerns.
- Highlight concerning searches and online behaviours.
- Support investigations.
- Assist with identifying incidents such as cyberbullying, harmful searches or attempts to bypass filtering systems.

The Headteacher is responsible for:

- Procuring filtering and monitoring systems.
- Reviewing effectiveness at least annually.
- Documenting decisions regarding filtering rules.
- Reporting arrangements to governors.

The DSL is responsible for:

- Reviewing monitoring reports.
- Managing safeguarding concerns arising from reports.
- Supporting regular reviews of effectiveness.
- Maintaining records of actions taken.

The IT service provider is responsible for:

- Maintaining technical systems.



- Producing monitoring reports.
- Supporting safeguarding investigations.
- Completing agreed actions following reviews.

Monitoring also includes active supervision of pupils by staff when using internet-enabled devices.

Education and Training

Online Safety Across the Curriculum

Online safety is taught through the Computing curriculum, PSHE, assemblies and wider safeguarding activities.

Pupils are taught about:

- Safe online behaviour.
- Privacy and personal information.
- Cyberbullying.
- Online relationships.
- Consent and respect.
- Misinformation and disinformation.
- Online scams and phishing.
- Reporting concerns.
- Digital wellbeing.
- Safe and responsible use of AI technologies.

Staff Training

All staff receive regular safeguarding and online safety training, including updates on emerging technologies and safeguarding risks.

New staff receive online safety information as part of their induction.

Governors receive appropriate safeguarding and online safety updates to enable them to fulfil their responsibilities.

Raising Parent and Carer Awareness

Online Safety information is provided through:

- Monthly Online Safety Newsletters.
- School website resources.
- Safeguarding communications.
- Parent information sessions where appropriate.



Standards and Inspection

The school evaluates the effectiveness of online safety arrangements through:

- Analysis of online safety incidents.
- Review of filtering and monitoring reports.
- Pupil and staff feedback.
- Safeguarding reviews.
- Governor monitoring.

New technologies, applications and AI systems will be risk assessed before implementation.

Online safety records, filtering arrangements and monitoring systems will be reviewed regularly and at least annually.

Policy amendments will be communicated to staff, governors, parents/carers and pupils as appropriate.

Signed: David Ashcroft, Headteacher

Date: September 2026

Review Date: September 2027

To be approved by the Finance, Resources & Staffing Committee on 03/11/2026