


# Online Safety Policy
# 2026–2027

*Grow Together; Learn Together; Feel Loved.*

| | |
|---|---|
| **Policy lead** | **Executive Headteacher / Designated Safeguarding Lead** |
| **Safeguarding governor** | Dr Nicky Shaw |
| **Approved** | October 2026 |
| **Next review** | Autumn 2027 or sooner following significant changes |

## 1. Purpose and principles

At Thurlstone Primary School, online safety is part of our commitment to Grow Together, Learn Together, Feel Loved. We want every child to feel safe, valued and included, both in school and when using technology beyond the school gates. Online safety is an integral part of safeguarding, teaching and school culture.
This policy explains how the school educates pupils, supports families and staff, and identifies, records and responds to online risks and harm. It applies to pupils, staff, volunteers, governors and users of school technology, including off-site use where relevant.

Our approach reflects our expectations to Be Ready, Be Respectful and Be Safe. We teach children to use technology responsibly, treat others with kindness and respect, and seek help when something online makes them feel worried or unsafe. We take a child-centred, inclusive and proportionate approach, considering children's developmental stage, SEND, disability, vulnerability and individual circumstances when responding to concerns.

We recognise that online harm may be a sign of wider safeguarding concerns. All concerns must be taken seriously and responded to promptly, so that children feel listened to, supported and protected.

## 2. Legal and guidance framework

This policy should be read alongside Thurlstone Primary School's Child Protection and Safeguarding Policy and reflects the school's wider safeguarding responsibilities.

The policy takes account of the following statutory guidance and relevant Department for Education guidance:

- *Keeping Children Safe in Education 2026*.
- *Working Together to Safeguard Children*.
- DfE *Filtering and monitoring: core standard*.
- DfE *Teaching Online Safety in Schools*.
- DfE guidance on *Generative artificial intelligence (AI) in education*.
- DfE *Generative AI: product safety standards*.
- DfE *Searching, Screening and Confiscation* guidance.
- DfE guidance on *Preventing and Tackling Bullying*, including cyber-bullying.

The policy also reflects relevant legislation, including:

- Education Act 2002.
- Education and Inspections Act 2006.
- Equality Act 2010.
- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

This policy should be read alongside the school's related policies and procedures, including the Behaviour and Relationships Policy, Anti-Bullying Policy, Mobile Technology Policy, acceptable-use arrangements, Data Protection Policy, Privacy Notices and Staff Code of Conduct.
The policy will be reviewed at least annually and sooner where necessary to reflect changes in statutory guidance, technology, safeguarding risks or school practice.

## 3. Understanding online risks

Online risks can be understood through four interrelated categories: **Content, Contact, Conduct and Commerce**. These categories help staff recognise potential risks and understand how online experiences may affect children's safety and wellbeing. A concern may involve more than one category.

- **Content:** Accessing or being exposed to harmful, illegal or age-inappropriate material, including extremist content, pornography, material promoting self-harm, misinformation and harmful or misleading AI-generated content.
- **Contact:** Unsafe contact with others online, including grooming, coercion, impersonation, harassment, exploitation and unwanted contact.
- **Conduct:** Online behaviour that harms others or places children at risk, including cyber-bullying, abusive messaging, unsafe disclosures, harmful sharing of images and the non-consensual creation or distribution of manipulated images.
- **Commerce:** Financial and commercial risks, including scams, phishing, inappropriate advertising, gambling-style features and financial exploitation.

Online risks can occur both in and out of school and may be an indicator of wider safeguarding concerns, including abuse, exploitation or vulnerability. All staff must remain alert to changes in children's behaviour, disclosures or patterns of concern that may indicate online harm. Concerns must be taken seriously, reported promptly to the Designated Safeguarding Lead (DSL) and managed in line with the school's safeguarding procedures.

In keeping with our expectations to **Be Ready, Be Respectful and Be Safe**, pupils are taught to make safe choices online, treat others respectfully and seek help from a trusted adult if something makes them feel worried, uncomfortable or unsafe.

## 4. Roles and accountability

Online safety is a shared safeguarding responsibility. Each role has clear responsibilities to ensure that risks are identified, concerns are reported, preventative education is delivered and appropriate action is taken.

**Governing body**
The governing body:

- Ensures the school meets its safeguarding responsibilities in relation to online safety.
- Approves this policy and monitors its implementation.
- Receives assurance about filtering and monitoring arrangements, significant risks, incidents and review actions.
- Ensures staff receive appropriate training.

**Named safeguarding governor: Dr Nicky Shaw**
The safeguarding governor:

- Reviews safeguarding and online-safety assurance with school leaders.
- Provides appropriate challenge and reports relevant matters to the governing body.
- Does not replace the operational responsibilities of school leaders or the DSL.

**Executive Headteacher responsible for filtering and monitoring: Mrs Charlotte Gibbins**
The Executive Headteacher:

- Ensures this policy is implemented effectively and online safety remains a priority within safeguarding.
- Oversees filtering and monitoring provision and ensures responsibilities and escalation routes are clear.
- Ensures risk-based decisions, exceptions and review actions are documented.
- Ensures staff have appropriate training and that identified concerns are addressed.
- Ensures online safety is embedded within the curriculum, safeguarding culture and wider school practice.
- Monitors the effectiveness of preventative work and identifies areas for improvement.

**Designated Safeguarding Lead (DSL) team: Charlotte Gibbins and Beth Wise; Deputy DSL: Nick Peace**
The DSL team:

- Leads the safeguarding response to online-safety concerns.
- Ensures concerns are recorded and assessed in line with safeguarding procedures.
- Reviews relevant CPOMS records and monitoring information, identifying patterns, emerging risks and any need for further action.
- Makes referrals to external agencies where appropriate.
- Advises staff on emerging online risks and how these may affect individual pupils or groups of children.
- Uses safeguarding concerns and identified patterns to inform preventative teaching, support and intervention.
- Provides safeguarding updates and assurance to school leaders and governors.

**Trust IT:**

- Maintains and supports the school's technical security, filtering and monitoring systems.
- Provides relevant monitoring reports and supports system testing and review.
- Implements authorised technical changes and addresses identified technical issues promptly.
- Works with school leaders to support effective filtering and monitoring arrangements.

Technical responsibility does not remove the school's accountability for safeguarding or for ensuring that concerns are acted upon.

**All teaching staff:**

- Deliver age-appropriate online safety education through relevant curriculum subjects, including computing, PSHE and relationships education, and reinforce these messages through everyday teaching and interactions.
- Teach pupils how to recognise risks, protect personal information, communicate respectfully, question online content and report concerns to a trusted adult.
- Adapt teaching and support to pupils' developmental stages, SEND and individual needs.
- Reinforce the school's expectations to **Be Ready, Be Respectful and Be Safe** in online as well as offline contexts.
- Report online-safety and safeguarding concerns promptly in line with school procedures.

**All staff and volunteers:**

- Follow this policy and the school's acceptable-use requirements.
- Supervise and support safe use of devices as appropriate to their role.
- Reinforce safe, responsible and respectful online behaviour.
- Report online-safety and safeguarding concerns promptly in line with school procedures.
- Maintain professional boundaries when using technology and communicating online.

**Parents and carers are encouraged to:**

- Reinforce safe and responsible use of technology at home.
- Talk with their children about their online experiences and encourage them to seek help if something worries them.
- Share online-safety concerns with the school.
- Engage with information and guidance provided by the school to support children's online safety.

## 5. Filtering, monitoring and technical safeguarding

Thurlstone Primary School will maintain appropriate filtering and monitoring arrangements to help safeguard pupils and staff. These arrangements will reflect pupils' ages, needs and risk profiles, the technology and services used in school, and emerging risks, including those associated with generative AI.
Filtering helps prevent access to illegal, inappropriate or potentially harmful content. Monitoring helps identify concerning activity so that it can be assessed and acted upon. Neither replaces effective adult supervision, teaching or the school's wider safeguarding procedures.

**Review and oversight**
Filtering and monitoring provision will be reviewed at least once every academic year and sooner where safeguarding risks, working practices, devices, systems or the use of new technology change significantly.
The review will involve senior leaders, the DSL, Trust IT or relevant technical support, and the responsible governor. It will consider the school's risk profile, pupil needs, filtering and monitoring coverage, use of devices and online services, relevant safeguarding concerns, technical limitations and the effectiveness of existing arrangements. Findings, decisions and actions will be documented.

**Monitoring, checks and reporting**
The school will ensure that:

- Named leads and responsibilities are clear, including who receives, reviews and acts on reports and how concerns are escalated.
- Monitoring arrangements include weekly reports highlighting incidents and immediate reports for high-risk incidents, in line with the DfE filtering and monitoring core standard.

- Filtering and monitoring are checked on school-managed devices and services, including devices used off-site, and that appropriate arrangements are in place for staff, pupils and guest accounts.
- Checks are recorded, including the date, person responsible, what was tested, the results and any remedial actions required.
- Changes to filtering and monitoring are authorised, documented and reviewed.
- Staff know how to report suspected access to harmful content, inappropriate restrictions, attempts to bypass filtering, system failures or other technical concerns to the appropriate school lead and technical support.
- Filtering and monitoring arrangements are reviewed when new devices, services or AI tools are introduced, including consideration of technical limitations and any additional safeguards required.

**Privacy and data protection**

Filtering and monitoring must be implemented lawfully and proportionately. The school will ensure that relevant privacy notices explain monitoring arrangements and that data protection impact assessments are completed where required, including where technical monitoring systems or new services involve the processing of personal data.

Identified safeguarding concerns will be referred to the DSL and managed in line with the school's safeguarding procedures. Technical issues will be raised with Trust IT or the relevant provider. Actions and outcomes will be recorded appropriately.

## 6. Responding to online safety concerns

All online-safety concerns must be reported promptly to the Designated Safeguarding Lead (DSL) or Deputy DSL and recorded in CPOMS in accordance with the school's Child Protection and Safeguarding Policy. Staff must not delay reporting while attempting to establish the facts or investigate the concern themselves.

Where a child is in immediate danger, staff must follow emergency safeguarding procedures and contact the emergency services where necessary. The DSL will assess the concern, consider the child's immediate safety and wider safeguarding needs, and determine appropriate action. This may include supporting the child, seeking advice, contacting parents or carers where appropriate, and making referrals to children's social care, the police or specialist agencies. Decisions, actions and outcomes must be recorded appropriately.

Staff must preserve relevant information where it is safe and appropriate to do so, but must not view, copy, forward, download or deliberately delete suspected indecent images of children. They must not ask a child to send or show images to them. Staff should secure the situation, avoid further sharing or access, and seek immediate guidance from the DSL, who will follow current safeguarding guidance and seek specialist advice where necessary.

Any searching of a pupil or their possessions, and any confiscation of a device, must be undertaken only by appropriately authorised staff and in accordance with current Department for Education guidance on *Searching, Screening and Confiscation*. Decisions must be lawful, proportionate and appropriately recorded, with the child's safety and welfare remaining the priority.

Online bullying, harassment, discriminatory behaviour and the harmful sharing of images will be addressed through the school's safeguarding procedures and Behaviour and Relationships Policy, as appropriate. Responses will consider the nature and seriousness of the incident, its impact on those affected, any repeated or wider pattern of behaviour, and the risk of further harm. The school will provide appropriate support, take proportionate action and consider restorative approaches where suitable and safe.

Throughout the process, the school will take a child-centred approach, ensuring that children are listened to, treated with dignity and supported without blame. Information will be shared with relevant people and agencies when necessary to safeguard children, in line with the school's safeguarding and data protection procedures.

## 7. Teaching pupils and working with families

Thurlstone Primary School will teach online safety progressively through computing, Relationships, Sex and Health Education (RSHE), PSHE, myHappymind, assemblies and relevant wider curriculum opportunities. Teaching will be age-appropriate and build pupils' knowledge and confidence as they move through the school.

Pupils will be taught how to protect personal information, understand privacy and consent, communicate respectfully, recognise and report concerns, evaluate online information, identify misinformation and manipulation, and recognise risks associated with online gaming, scams and the use of artificial intelligence (AI). Teaching will help pupils understand that their online actions can affect themselves and others, and that they should seek help from a trusted adult whenever something online makes them feel worried, uncomfortable or unsafe.

Teaching and support will be adapted where necessary to reflect pupils' developmental stages, SEND, communication needs and other vulnerabilities, so that all pupils can access and apply the guidance.

The school will work in partnership with parents and carers to promote safe and responsible technology use beyond the school gates. Accessible guidance and information will be shared through appropriate school communication channels, including the school website, newsletters, workshops and Class Dojo. Families will be signposted to relevant advice and informed about the school's filtering and monitoring arrangements and how to report online-safety concerns.

Staff will listen to children who share concerns and respond in a calm, supportive and non-judgemental manner. Staff must not promise absolute confidentiality when a child makes a safeguarding disclosure. They must explain, in an age-appropriate way, that information may need to be shared with the DSL or other appropriate people to help keep the child or others safe.

## 8. Devices, communication and acceptable use

Pupils' mobile phones and connected devices will be managed in accordance with the school's current Mobile Technology Policy. This Online Safety Policy must not be interpreted as permitting arrangements that conflict with that policy.

Staff must use approved school systems for school business and follow the school's expectations for professional communication with pupils and families. Staff are responsible for protecting their accounts, passwords and devices, and must follow school requirements relating to personal devices, photography, recording, messaging and online communication. Personal accounts and communication channels must not be used in ways that compromise professional boundaries or safeguarding.

School-managed devices used off-site remain subject to the relevant security and safeguarding controls. Staff must take appropriate steps to protect devices and information from loss, unauthorised access or inappropriate use, and report any suspected security breach or safeguarding concern promptly.

Age-appropriate acceptable-use agreements for pupils, staff and governors will be kept current, accessible and communicated to the relevant users. These agreements will set out expectations for safe, responsible and respectful use of school technology and online services.

Any remote-learning arrangements or approved use of personal devices for school purposes must be risk assessed, clearly communicated and managed in line with relevant school policies and safeguarding, data protection and security requirements. Concerns arising from device use or online communication must be reported and managed in accordance with the school's safeguarding procedures.

## 9. Generative AI and emerging technology

Thurlstone Primary School will consider the safeguarding, educational and data protection implications of generative artificial intelligence (AI) and other emerging technologies. Any proposed AI product must be assessed and approved before it is used by pupils or staff for school purposes.

Risk assessments will consider safeguarding risks, privacy and data protection, age suitability, accuracy, bias, filtering and monitoring capability, and the safeguards provided by the supplier. Any use must be appropriate to the intended purpose and consistent with the school's safeguarding, acceptable-use and data protection requirements.

Pupils may use only school-approved AI tools under appropriate adult supervision. Staff and pupils must not enter identifiable or confidential pupil information, personal data or other sensitive school information into unapproved AI tools.

Online safety education will help pupils recognise the risks associated with AI-generated content, including synthetic images and videos, deepfakes, impersonation, misinformation and misleading or harmful material. Pupils will be encouraged to question what they see online, consider the reliability of information and treat others respectfully.

Any concern involving AI-generated harmful content, impersonation, exploitation, bullying or other online harm must be reported promptly to the DSL and recorded in CPOMS in accordance with the school's safeguarding procedures. The school will assess the risk and take appropriate action, following the same safeguarding principles and escalation procedures used for other online-safety incidents..

## 10. Training, monitoring and review

All staff will receive online-safety information as part of induction, annual safeguarding updates and further briefings when risks, technology or procedures change. Training will help staff recognise online risks, understand their responsibilities and know how to report and respond to concerns.

Governors will receive safeguarding and online-safety training appropriate to their responsibilities, enabling them to provide effective oversight and challenge. The DSL will ensure that learning from incidents, emerging risks and changes in guidance informs safeguarding practice, staff updates and pupil education, as appropriate.

This policy will be reviewed at least annually and sooner following significant incidents, changes in statutory guidance, emerging risks or changes to school practice or technology.

The governing body will receive an annual assurance summary covering staff training, online-safety education, filtering and monitoring reviews, significant trends, actions taken and outstanding risks. Pupil and family views will inform the review and ongoing improvement where appropriate. Actions arising from reviews, incidents or identified weaknesses will be recorded, assigned to appropriate leads and followed up to ensure that improvements are implemented.