Thringstone
Primary School

Believe and Achieve Together

Online Safety

Approved by the Governing Body:

Adopted on: November 2025

Review November 2026

Vision and Values

At Thringstone Primary School, our vision is **Believe and Achieve Together**.

Our five core values - **Belief, Respect, Kindness, Resilience and Teamwork** - underpin everything we do. They guide how we teach, learn and interact both in person and online. This policy reflects those values by promoting respect, responsibility and safety across all areas of digital life.

1. Aims

Thringstone Primary School aims to:

- Keep all children, staff, volunteers and governors safe when using technology.
- Promote safe, responsible and positive use of digital tools in school and at home.
- Ensure clear systems are in place to identify, respond to and escalate online concerns.
- Educate our whole school community about how to use technology safely and respectfully.

Our approach is based on the four recognised categories of online risk:
Content – exposure to harmful or inappropriate material such as pornography, extremism or misinformation.
Contact – harmful online interactions such as grooming, pressure or exploitation.
Conduct – behaviour that causes harm, such as bullying, sexting or sharing explicit material.
Commerce – risks such as scams, gambling or phishing.

2. Legislation and Guidance

This policy is based on current Department for Education guidance including:

- Keeping Children Safe in Education (2025)
- Teaching Online Safety in Schools
- Preventing and Tackling Bullying (including Cyberbullying)
- Searching, Screening and Confiscation
- The Prevent Duty

It reflects the requirements of the Education Act 1996, the Education and Inspections Act 2006, the Education Act 2011 and the Equality Act 2010.

3. Roles and Responsibilities

Headteacher

The Headteacher has overall responsibility for online safety, ensuring that:

- The policy is implemented and understood by all staff.
- Training and updates are delivered regularly.

- Online safety incidents are managed and recorded through CPOMS.
- Systems for filtering and monitoring are in place and reviewed.

The Headteacher is also the Designated Safeguarding Lead (DSL).

Designated Safeguarding Leads

There are five trained safeguarding leads: Headteacher, Deputy Headteacher, Pre-School Manager, SENDCo and KS2 Phase Lead. They work together to:

- Log, investigate and respond to online safety concerns.
- Support staff, children and families in managing incidents.
- Liaise with external agencies when required.

ICT Provider

ICT Independent Consulting oversees:

- Filtering, monitoring and security across the school network.
- Regular checks to ensure compliance with DfE standards.
- Advice and support on system integrity and protection against viruses or malware.

All Staff and Volunteers

All staff are responsible for:

- Understanding and following this policy.
- Modelling safe, respectful online behaviour.
- Following the Staff Acceptable Use Agreement.
- Reporting any concerns to a safeguarding lead immediately.

Parents and Carers

Parents and carers are encouraged to:

- Support their child in using the internet responsibly.
- Read and sign the Parent and Child Acceptable Use Agreement.
- Raise any concerns with the class teacher or Headteacher.

Governing Board

The governing board:

- Holds the Headteacher to account for online safety provision.
- Reviews the policy annually as part of the safeguarding suite.
- Ensures systems, staff training and parental communication are in place.

4. Educating Children about Online Safety

Online safety is taught through the computing and PSHE curriculum and reinforced in assemblies, class discussions and themed events.

By the end of primary school, children will understand:

- How to use technology safely, respectfully and responsibly.
- How to protect personal information.
- How to report concerns about content or contact.

- That online actions have real consequences.
- How data and digital footprints are created and used.

Teaching is adapted to meet the needs of vulnerable children and those with SEND.

5. Educating Parents and Carers

Parents are kept informed about online safety through:

- ClassDojo posts and school newsletters.
- Updates on the school website.
- Information evenings or targeted communications if issues arise.

Information shared includes advice on filters, social media, gaming and supporting children to use technology safely.

6. Cyberbullying

Cyberbullying is bullying that takes place online or via electronic communication. The school teaches children what cyberbullying is, how to recognise it, and how to seek help. All reports are taken seriously and investigated in line with the Behaviour Policy.

Where appropriate, incidents will be reported to the police and external agencies. Any illegal or harmful material identified will be contained and reported through safeguarding channels.

7. Acceptable Use of the Internet and Technology

All children, staff, governors and volunteers must use the school's network and internet responsibly. School devices and systems are provided for educational purposes. The school monitors network use to ensure safety and compliance. Details are set out in the Acceptable Use Agreements.

8. Use of Mobile Devices

Children should not bring mobile phones or smart watches into school. Where this is unavoidable, the device must be handed into the school office on arrival and collected at the end of the day.

Staff issued with laptops or iPads may use them at home for work purposes only. Devices must be password-protected, stored securely and not shared with family members.

9. Responding to Misuse

Any misuse of school technology or internet access will be handled proportionately:

- Children – behaviour and safeguarding procedures will be followed.
- Staff – issues will be managed under the Staff Code of Conduct or Disciplinary Policy.

Serious incidents involving illegal material or behaviour will be reported to the police and safeguarding partners.

10. Training

All staff receive online safety training as part of annual safeguarding updates. New staff are trained during induction. Training includes recognising online risks, understanding reporting procedures and supporting children to stay safe online.

Governors and volunteers receive awareness training as appropriate.

11. Monitoring and Review

Online safety concerns are logged on CPOMS. Filtering and monitoring systems are reviewed regularly with ICT Independent Consulting. The Headteacher and safeguarding leads review incidents and patterns termly. The governing board reviews the policy annually or earlier if statutory guidance changes.

12. Related Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection and Privacy Notices
- Complaints Procedure

Appendix A:

Thringstone
Primary School
Believe and Achieve Together

Staff, Governor and Volunteer Acceptable Use Agreement

When using school ICT systems, devices or the internet, I will:

- Use school devices and accounts for professional purposes only.
- Protect my passwords and keep all confidential data secure.
- Ensure any device used off-site is stored safely, password-protected and used only by me.
- Not access, download or share inappropriate material.
- Not use personal social media, messaging or personal email to communicate with children.
- Report any safeguarding, security or data breaches immediately.
- Take care when publishing or sharing school-related information online.
- Use only school-approved platforms for communication such as ClassDojo or school email.

I understand that the school may monitor use of its systems and devices. I will uphold the standards set out in this agreement and the Staff Code of Conduct.

Signed: ____________________________

Name: ____________________________

Role: ____________________________

Date: ____________________________

Appendix B:

Thringstone
Primary School
Believe and Achieve Together

Parent and Child Acceptable Use Agreement

When I use the computers, tablets or the internet at school, I will:

- Use them safely and respectfully.
- Tell an adult if something online worries or upsets me.
- Never share my full name, address or passwords.
- Only go on websites or apps my teacher has said are safe.
- Be kind and polite online.
- Look after the equipment and not change settings or install anything.

I understand that if I do not follow these rules, I may lose my computer privileges.

Parent/Carer Agreement

I have read and discussed this agreement with my child and support the school's approach to safe internet use. I understand that the school monitors online activity to protect all users.

Parent/Carer Signature: ___________________________

Parent/Carer Name: ___________________________

Date: ___________________________

Child's Name: ___________________________