



HOLY TRINITY CE PRIMARY SCHOOL & PRE-SCHOOL

Learning together with God's love

We aspire to be a happy, confident and caring community where children flourish

Perseverance Aspiration Respect Teamwork

1 Corinthians 16:14 Do everything in love

Online Safety Policy

REVIEWED BY	SLT; FGB
APPROVED	16.09.26
REVIEW DUE	Autumn 2027

1. Aims

Holy Trinity CE Primary School is committed to safeguarding and promoting the welfare of all pupils. The purpose of this policy is to:

- Protect children and young people from harm when using digital technologies.
- Provide staff and volunteers with principles that guide safe and responsible use of technology.
- Ensure online safety is embedded as a running and interrelated theme throughout safeguarding practice.
- Establish clear procedures for preventing, identifying and responding to online safety concerns.
- Promote positive, responsible and educational use of technology by pupils, staff and parents.

This policy should be read alongside the Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, Data Protection Policy, Mobile Phone Policy and, where applicable, the school's Artificial Intelligence (AI) Usage Policy.

2. Legislation and Guidance

This policy has regard to:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- UK GDPR and Data Protection Act 2018

- The Education Act 2002
 - The Online Safety Act
 - Searching, Screening and Confiscation Guidance
 - Meeting Digital and Technology Standards in Schools and Colleges
 - Mobile Phones in Schools Guidance
 - The Children's Wellbeing and Schools Act 2026
 - Prevent Duty Guidance
-

3. Roles and Responsibilities

Governing Body

The Governing Body will ensure that:

- Online safety is a strategic safeguarding priority.
- Appropriate filtering and monitoring systems are in place and effective.
- Filtering and monitoring arrangements are reviewed annually.
- Online safety risks are considered in all safeguarding decisions.
- Staff receive regular training.
- The school complies with relevant legal requirements.

Headteacher

The Headteacher will:

- Ensure this policy is implemented effectively.
- Ensure appropriate filtering and monitoring systems are maintained.
- Ensure robust safeguarding arrangements are in place when the DSL is unavailable.
- Ensure online safety incidents are investigated and managed appropriately.
- Promote a culture of safe and responsible technology use.

Designated Safeguarding Lead (DSL)

The DSL will:

- Take lead responsibility for online safety.
- Receive and manage online safety concerns.
- Liaise with external agencies where required.
- Monitor trends and emerging risks.
- Provide assurance to governors regarding filtering and monitoring effectiveness.

- Respond to safeguarding alerts generated through filtering and monitoring systems.
- Ensure online safety is embedded within safeguarding training and curriculum delivery.

Staff

All staff will:

- Maintain an up-to-date understanding of online safety risks.
- Follow acceptable use agreements.
- Report safeguarding concerns immediately.
- Model safe and responsible technology use.
- Teach online safety through curriculum opportunities.

4. Online Safety Education

4.1 Educating Pupils

Online safety education is delivered through the curriculum, assemblies, themed activities and pastoral support.

Pupils will be taught about:

Content Risks

- Illegal, harmful or inappropriate content.
- Violent, extremist and hateful material.
- Misinformation, disinformation and conspiracy theories.
- AI-generated content and deepfakes.
- Inappropriate advertising and online influence.

Contact Risks

- Online grooming.
- Peer pressure and coercion.
- Online strangers.
- Social media contact.
- AI chatbots and applications that simulate human interaction.

Conduct Risks

- Cyberbullying.
- Sharing personal information.
- Creating and sharing harmful content.

- AI-generated inappropriate images.
- Online harassment and abuse.
- Responsible digital citizenship.

Commerce Risks

- Online scams.
- Fraud.
- Phishing attacks.
- In-app purchases.
- Financial exploitation.

Pupils will also learn:

- Minimum age requirements for social media platforms.
- How to identify fake accounts and online identities.
- Safe privacy settings.
- Location sharing risks.
- Digital footprints and the permanence of online content.
- Reporting concerns and seeking support.

4.2 Practical Cyber Security Skills

Pupils will receive age-appropriate education regarding:

- Password security.
- Secure logins.
- Multi-factor authentication.
- Device security.
- Social engineering.
- Cyber scams.
- Safe downloading.
- Protecting personal information.
- Reporting cyber incidents.

5. Filtering and Monitoring

The school will maintain filtering and monitoring systems that:

- Protect children from harmful online content.

- Alert appropriate staff to safeguarding concerns.
- Support compliance with statutory safeguarding requirements.
- Are regularly reviewed for effectiveness.
- Are appropriate to the age and needs of pupils.

Filtering and monitoring arrangements will be reviewed at least annually and whenever significant technological changes occur.

6. Artificial Intelligence (AI)

The school recognises the growing use of Artificial Intelligence technologies.

AI may provide educational benefits but also presents safeguarding risks.

The school will:

- Assess risks before introducing AI tools.
- Monitor developments in AI technology.
- Educate pupils about safe and ethical AI use.
- Ensure safeguarding and personal data are protected.

Pupils will be taught about:

- Deepfakes.
- AI-generated misinformation.
- Manipulated media.
- AI-generated indecent images.
- Risks associated with sharing information with AI systems.

Staff must not enter:

- Personal pupil data.
- Safeguarding information.
- Confidential school information.
- Personnel information.

into publicly available AI systems unless specifically approved and compliant with data protection requirements.

7. Mobile Phones

Holy Trinity CE Primary School operates a mobile-phone-free environment.

Where a pupil requires a mobile phone for travel to and from school:

- The device must remain switched off upon arrival.
- The device must be handed to the school office immediately.
- The phone must not be accessed during the school day.
- The phone will be returned at the end of the school day.

Staff mobile phone use must comply with safeguarding and professional conduct expectations.

8. Cyberbullying

Cyberbullying will not be tolerated.

Incidents may include:

- Offensive messages.
- Harassment.
- Distribution of images.
- Exclusion from online groups.
- Impersonation.
- Threatening behaviour.

All incidents will be investigated and managed in accordance with the Behaviour and Safeguarding Policies.

9. Use of Images and Videos

The school will:

- Obtain appropriate permissions where required.
 - Store images securely.
 - Use images only for approved educational and school purposes.
 - Prevent unauthorised sharing of pupil images.
-

10. Searching, Screening and Confiscation

Where a member of staff believes a device contains harmful, illegal or inappropriate material, action will be taken in accordance with statutory guidance.

If staff believe a device contains a nude or semi-nude image of a child, they must:

- Not view the image.
- Not forward or copy the image.
- Not save the image.

- Not delete the image.
- Not ask the child to share the image.
- Refer immediately to the DSL.

This includes concerns regarding AI-generated indecent images.

11. Staff Use of Technology

Staff must:

- Use only authorised accounts and systems.
- Maintain secure passwords.
- Follow National Cyber Security Centre guidance.
- Keep devices updated.
- Use anti-virus protection.
- Use anti-spyware protection where appropriate.
- Protect confidential information at all times.

Staff must not:

- Share passwords.
 - Use personal devices for confidential information unless authorised.
 - Circumvent school security systems.
 - Share safeguarding information through unauthorised platforms.
-

12. Training

All staff will receive regular online safety training.

Training will include:

- Emerging online risks.
- AI-generated content.
- Deepfakes and deepnudes.
- Cyber security.
- Filtering and monitoring responsibilities.
- Social media risks.
- Data protection requirements.
- Child-on-child abuse online.

Governors will receive appropriate online safety training relevant to their responsibilities.

13. Working with Parents and Carers

The school will support parents by providing information about:

- Online risks and trends.
 - Social media safety.
 - Filtering and monitoring systems used by the school.
 - Digital wellbeing.
 - Cyber security.
 - Appropriate use of AI technologies.
 - Online platforms pupils may be asked to access.
-

14. Monitoring and Review

This policy will be reviewed annually or sooner if:

- Legislation changes.
- National guidance changes.
- Significant safeguarding issues emerge.
- New technologies present additional risks.

The Governing Body is responsible for approving the policy and monitoring its implementation.

Appendix 1: Pupil Acceptable Use Agreement

Pupils will:

- Use technology responsibly.
 - Keep passwords secure.
 - Report concerns to a trusted adult.
 - Be respectful online.
 - Use AI tools only when permitted by staff.
 - Not create or share harmful content.
 - Protect personal information.
-

Appendix 2: Parent Acceptable Use Agreement

Parents and carers are expected to:

- Support safe technology use at home.
- Monitor their child's online activity appropriately.
- Follow school expectations regarding mobile phones.
- Support responsible use of AI technologies.
- Report concerns promptly.

Appendix 3: Staff Acceptable Use Agreement

Staff will:

- Use school systems professionally and securely.
- Follow safeguarding and data protection requirements.
- Use AI appropriately and responsibly.

Staff must not enter into public AI tools:

- Pupil personal information.
- Safeguarding records.
- Child protection information.
- Confidential school business information.
- Personnel information.

Failure to comply may result in disciplinary action.

Policy Review Date: September 2027

Approved By: Governing Body

Responsible Lead: Designated Safeguarding Lead and Headteacher