Holy Trinity Church of England Primary School

Online Safety Policy

'Loved by God and one another, Holy Trinity is a welcoming community of faith, where we learn and flourish together.

Each day opens up horizons of hope, aspiration and joy!'

Agreed by staff	13.03.2026	
Ratified By Academy Council	18.03.2026	
Shared with Parents	19.03.2026	
Policy Revisit	September 2026	
Policy Review	01.03.2026	

Online Safety Policy

1. Rationale and Aims

Rationale

At Holy Trinity Church of England School, we are committed to fostering a welcoming community of faith where all children learn and flourish. We recognize that the online world is an integral part of lifelong learning, beginning in early childhood. This policy ensures a safe digital environment rooted in our core values of respect, love, and openness, supporting families as we navigate the opportunities and responsibilities of the 21st century together.

Aims of our Online Safety Policy

Holy Trinity Church of England Primary School aims to:

- ✓ Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- ✓ Identify and support groups of pupils that are potentially at greater risk of harm online than others
- ✓ Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- ✓ Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance,

Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education (RSE) and health education

Searching, screening and confiscation

This policy also refers to the DfE's guidance on protecting children from radicalisation.

This policy reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy also takes into account the National Curriculum computing programmes of study.

This policy complies with all Leeds Diocesan Learning Trust policies and articles of association

3. Roles and responsibilities

3.1 The Local Academy Council (LAC)

The LAC has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The LAC will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The LAC will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The LAC will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The LAC will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The LAC will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- ✓ Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- ✓ Reviewing filtering and monitoring provisions at least annually
- ✓ Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- ✓ Having effective monitoring strategies in place that meet the school's safeguarding needs

The governors who oversees online safety are Adam Kitching and Phil Carman

All governors will:

- ✓ Make sure they have read and understand this policy
- ✓ Agree and adhere to the terms on acceptable use of the Trust ICT systems and the internet
- ✓ Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- ✓ Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

The Headteacher takes lead responsibility for online safety in school, in particular

- ✓ Responsibility for managing the school Monitoring and Filtering Policy.
- ✓ Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- ✓ Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly

- ✓ Working with the ICT manager to make sure the appropriate systems and processes are in place
- ✓ Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's Designated Safeguarding Lead (DSL) Deputy Designated Safeguarding Lead (DDSL)are set out in our child protection and safeguarding policy, as well as DLS and DDLS job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- ✓ Supporting the headteacher and school leaders in making sure that all staff understand this policy and that it is being implemented consistently throughout the school
- ✓ Working with the headteacher and LAC to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- ✓ Working with the headteacher, Primary ICT and other staff, as necessary, to address any online safety issues or incidents
- ✓ Managing all online safety issues and incidents in line with the school's Child Protection Policy
- ✓ Responding to safeguarding concerns identified by filtering and monitoring
- ✓ Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- ✓ Updating and delivering staff training on online safety (appendix 2 contains a self-audit for staff on online safety training needs)
- ✓ Liaising with other agencies and/or external services if necessary
- ✓ Providing regular reports on online safety in school to the headteacher and LAC
- ✓ Undertaking annual risk assessments that consider and reflect the risks pupils face
- ✓ Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

3.4 The ICT Manager (Primary ICT)

The ICT manager is responsible for:

- ✓ Putting in place an appropriate level of security protection procedures, such as Securly (filtering and monitoring systems) on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ✓ Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- ✓ Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- ✓ Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- ✓ Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- ✓ Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- ✓ Maintaining an understanding of this policy
- ✓ Implementing this policy consistently
- ✓ Agreeing and adhering to the terms on acceptable use of the Trust ICT systems and the internet and making sure that pupils follow the school's terms on acceptable use (appendix 1)

- ✓ Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by [insert school specific action here]
- ✓ Following the correct procedures by [insert school specific action here] if they need to bypass the filtering and monitoring systems for educational purposes
- ✓ Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- ✓ Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- ✓ Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

3.6 Parents/carers

Parents/carers are expected to:

- ✓ Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- ✓ Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- ✓ What are the issues? – UK Safer Internet Centre
- ✓ Help and advice for parents/carers – Childnet
- ✓ Parents and carers resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

The text below is taken from the National Curriculum computing programmes of study and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for introduction 1 September 2026)
All schools have to teach:
Relationships education and health education in primary schools
Relationships and sex education and health education in secondary schools

At Holy Trinity in EYFS & Key Stage (KS1) pupils will be taught to:

- ✓ Use technology safely and respectfully, keeping personal information private
- ✓ Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

At Holy Trinity pupils in Key Stage (KS2)will be taught to:

- ✓ Use technology safely, respectfully and responsibly
- ✓ Recognise acceptable and unacceptable behaviour
- ✓ Identify a range of ways to report concerns about content and contact
- ✓ Be discerning in evaluating digital content
- ✓ By the end of primary school, pupils will know:

- ✓ That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- ✓ How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- ✓ That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- ✓ The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- ✓ Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- ✓ That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online.

At Holy Trinity

- ✓ The safe use of social media and the internet will also be covered in other subjects where relevant.
- ✓ Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

At Holy Trinity we will raise parents/carers' awareness of internet safety in school hosted workshops, letters or other communications home, and in information via our website or virtual learning environment This policy will also be shared with parents/carers.
Online safety will also be covered during parents' evenings.
The school will let parents/carers know:

- ✓ What systems the school uses to filter and monitor online use
- ✓ What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class Teachers will discuss cyber-bullying with their cohort at an age appropriate level.

All staff will use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, or any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- ✓ Poses a risk to staff or pupils, and/or
- ✓ Is identified in the school rules as a banned item for which a search can be carried out, and/or
- ✓ Is evidence in relation to an offence

Staff will not access information on pupils owned electronic device without a parent present.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Holy Trinity Church of England Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used inappropriately For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Holy Trinity Church of England Primary School will treat any use of AI to harm pupils very seriously, in line with our Antibullying Policy
Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the Holy Trinity Church of England Primary School, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors who access the school internet are expected to sign the LDLT Acceptable Use Policy regarding the acceptable use of the school's ICT systems and the internet (appendix 1). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils, staff, volunteers, governors and visitors) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school. Pupils are required to turn oof all devices as they enter the school playground but are not permitted to use them whilst on school premises unless they have specific permission from a member of staff

Any breach of the acceptable use agreement by a pupil may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- ✓ Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- ✓ Making sure the device locks if left inactive for a period of time
- ✓ Not sharing the device among family or friends

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in the LDLT Acceptable Use Policy.
Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from Primary ICT

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and Acceptable The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with LDLT staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- ✓ Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- ✓ Children can abuse their peers online through:
- ✓ Abusive, threatening, harassing and misogynistic messages

- ✓ Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- ✓ Sharing of abusive images and pornography, to those who don't want to receive such content
- ✓ Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- ✓ Develop better awareness to assist in spotting the signs and symptoms of online abuse
- ✓ Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- ✓ Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety annually. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- ✓ Methods that hackers use to trick people into disclosing personal information
- ✓ Password security
- ✓ Social engineering
- ✓ The risks of removable storage devices (e.g. USBs)
- ✓ Multi-factor authentication
- ✓ How to report a cyber incident or attack
- ✓ How to report a personal data breach
- ✓ Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS. Logs of internet breaches can be found on the school's Securly report log.

This policy will be reviewed annually by the headteacher and DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- ➢ Safeguarding and Child Protection Policy
- ➢ Behaviour Policy
- ➢ LDLT Staff disciplinary procedures
- ➢ Data protection policy and privacy notices
- ➢ LDLT Complaints Procedure
- ➢ LDLT Acceptable Use Policy

Acceptable Use Agreement for Key Stage One Pupils

Acceptable use of the school's computing and technology equipment and online services

Name	Class

When I use the school's ICT (like computers and equipment) and when I go on the internet, I will:

- ask an adult first and make sure an adult is in the room with me
- keep my passwords safe and not tell anyone except my teacher or parents
- only send messages using the school's systems like TEAMS or Google Classroom, or systems that an adult in school tells me are safe
- be kind and respectful when working on the computers and sending messages
- never use mean or rude words when talking to other people using computers or other devices
- tell an adult in school immediately if I see something that I don't like, I know is wrong, or anything that makes me feel sad
- not open any attachments in emails, or click any links in emails, without checking with an adult first
- not share any photos or videos of people (including me) online
- carefully follow the instructions I am given by the adults in school
- only use the internet to search for things I have been told to look for and that I have been told are safe
- not use social media or social networking sites at school, because they are not meant for children and can be unsafe. I will tell an adult straight away if I see social media on a school device or if someone asks me to use it
- not use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me.

I know…

- I am responsible for making the right choices with technology, which will make it a useful and enjoyable tool for everyone
- it is not safe to talk to people I don't know online and that I mustn't tell people my personal information like my name or where I live
- school will speak with my parents if I make the wrong choices whilst using technology
- to tell a teacher or a member of staff immediately if I find anything on a school computer or online that upsets me, or that I know is unkind or wrong
- school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following safety rules.

I understand and follow these steps so that I learn as much as I can while using technology in school and I keep myself and others safe.

Signed (pupil):	Date:

Parent/carer agreement: I accept my child can use the school's ICT systems and internet, appropriately supervised by a member of school staff. I understand the school has a filtering system to block inappropriate websites. I accept the conditions set out above for pupils using the school's ICT systems and internet.

Signed (parent):	Date:

Acceptable Use Agreement for Key Stage Two Pupils

Acceptable use of the school's computing and technology equipment and online services

Name	Class

When using computing equipment in school, I will:

- use computers, the internet and any technology equipment that I am given to support my learning responsibly and in the way that the adults in school ask me
- seek permission from an adult to use school equipment or access the internet and websites that have been shared with me by an adult in school and that I have been told are safe
- only use school systems to communicate safely online e.g. Teams, Google Classroom
- tell an adult straight away if I see social media on a school device or if someone asks me to use it
- always act respectfully using appropriate language when communicating online or when using technology in school
- seek the permission of an adult to search for and add images to anything I create
- always look after my own computer and online safety by creating strong passwords and keeping them safe. I will only share my password with my teacher or parents.

When using computing equipment in school, I will not:

- access social networking sites or chat rooms at school (unless my teacher has expressly allowed this as part of a learning activity)
- share any images, videos or livestreams, even if I have the consent of the person or people in the photo
- share my password with others or log in to the school's network using someone else's details
- use any personal devices from home e.g. smart phones and watches
- view or share violent content
- open any attachments in emails, or follow any links in emails, without first checking with a teacher
- use any inappropriate language when communicating online, including in emails
- use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work.

I understand that the school will monitor the websites I visit and my use of the school's facilities and systems. I will immediately let a member of staff know if I find any material which might upset, distress or harm me or others. I understand that school will speak with my parents if I do unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	Date:

Parent/carer agreement: I accept that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I understand the school has a filtering system to block inappropriate websites. I accept the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

Signed (parent):	Date:

Appendix 2

HOLY TRINITY CHURCH OF ENGLAND SCHOOL ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	