Holy Trinity Primary School Online Safety Policy

Key people / dates

Holy Trinity R.C. Primary School	**Headteacher/Designated Safeguarding Lead**	**Mrs M Lyle**
	Deputy Headteacher/Deputy Designated Safeguarding Lead	**Mr M McManus**
	Online-safety / safeguarding link governor	**Mr P Simm**
	Pastoral manager /Deputy Designated Safeguarding Lead	**Mrs K Clowes**
	PSHE/RSE lead	**Mr M McManus**
	ICT technician	**Mr John Kavanagh**
	Computing subject lead	**Mrs M Lyle**
	Date this policy was reviewed and by whom	**July 2025** **Mrs K Clowes**
	Date of next review	**September 2025**

Mission Statement

To go forward together in Christ, respecting our neighbour and striving for excellence.

Introduction

Purpose and Scope: Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. This policy outlines the standards and procedures for safe online conduct and usage within our school. It applies to all members of Holy Trinity R.C. Primary School including: all students, staff, volunteers, parents/carers, and visitors engaging with school's digital platforms and technologies.

Rational: Engaging with digital technologies is an integral part of our learning in our school; however, this comes with potential risks. This policy establishes guidelines to ensure a safe online environment and promote responsible digital citizenship. Accordingly, this policy is written in line with the relevant legislation and guidance listed below.

Legal Framework:

- The Children Act 1989 and 2004
- The Education Act 2002
- The Protection of Freedoms Act 2012
- Keeping Children Safe in Education (KCSIE) 2024
- Working Together to Safeguard Children
- Prevent Duty Guidance

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Available in paper format in the office
- Part of school induction pack for all new staff (including temporary, supply and nonclassroom based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)

Role	Key Responsibilities
Headteacher	• To take overall responsibility for online safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious online safety incident. • To receive regular monitoring reports from the Online safety Coordinator • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager)

Designated Safeguarding Lead	• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that online safety education is embedded across the curriculum
	• Liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated online safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
	• To ensure that an online safety incident log on CPOMs is kept up to date
	• Facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Role	Key Responsibilities
PSHE/RSHE Lead	As listed in the 'all staff' section, plus • Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives." • This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. • Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
Governors /Online safety governor	• To ensure that the school follows all current online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor - • To support the school in encouraging parents and the wider community to become engaged in online safety activities
Computing Curriculum Leader	• As listed in the 'all staff' section plus: • To oversee the delivery of the online safety element of the Computing curriculum • Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing • Ensure subject specific action plans also have an online-safety element

ICT technician	• To report any online safety related issues that arises. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web filtering is applied and updated on a regular basis • To keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of the *network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Head teacher for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • To keep up-to-date documentation of the school's e-security and technical procedures

Role	Key Responsibilities
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To ensure that pupils in EYFS/KS1 use the correct year group passwords and that pupils in KS2 use their individual passwords when accessing technology in school. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

All staff	• To read, understand and help promote the school's online safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of online safety policies

Parents/carers	• To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Education and Curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils) Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites. Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying,

Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Ongoing professional development is provided to all staff to handle online safety issues effectively and to stay updated with the latest online threats and safety protocols. Our Computing curriculum follows the Teach Computing scheme of work, Project Evolve is incorporated within the scheme and the key stages to ensure full coverage of online safety for pupils to focus on the principles of secure and responsible online behaviour. Information and resources are also provided to assist parents/carers in understanding the online risks and the strategies used by the school to mitigate them.

Infastructure and Filtering and Monitoring

This school:

- Has the educational filtered secured broadband connectivity;
- Uses Netsweeper filtering and monitoring system which blocks and restricts pupils from inappropriate content that may fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. This is provided by our local education authority;
- Three users have access to the filtering system, these users are: DSL / Headteacher, Business manager and the ICT technician – John Kavanagh. These accounts have the ability to login into the web filter and block or unblock specific websites.
- Daily reporting is enabled through this system and the features sends reports to the Headteacher and pastoral Manager's email addresses. These reports are the UK prevent report and the suspicious search query report.
- Monitoring is vigilant during lessons by the class teachers and all juniors have an individual log in so school can identify users.
- Ensures a healthy network through the use of anti-virus software and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA secured email to send personal data over the internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform; ○ Uses security time-outs on Internet access - practical / useful.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship. General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw

puzzle, so all stakeholders should err on the side of talking to the online safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence). School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes. Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's, Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of onlinesafety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and up skirting; see section below).

Incident Management

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.

- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

Software/hardware

- School has legal ownership of all software (including apps on tablet devices).
- School keeps an up to date record of appropriate licenses for all software. This is maintained by the IT Technician.
- An annual audit of equipment and software is made, this is then shared with the Governors and the Asset Register.
- The IT technician, Computing Co-ordinator and headteacher control what software is installed on school systems. Managing the network and technical support
- Any servers, wireless systems and cabling are securely located and physical access is restricted.
- All wireless devices have been security enabled and are accessible through a secure password.
- Relevant access settings should be restricted on tablet devices e.g. downloading of apps and purchases.
- School systems are kept up to date regularly in terms of security e.g. computers are regularly updated with critical software updates/patches.
- Staff are reminded to lock or log out of a school system when a computer/digital device is left unattended.
- Users can report any suspicion or evidence of a breach of security to the Computing Co-ordinator, IT Technician or the Headteacher.

Online Safety- Across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' online safety. Holy Trinity R.C Primary School provides relevant, flexible and engaging Online Safety education to all children as part of their curriculum entitlement.

- Termly Online Safety strands and topics to be covered in each year group during computing and/or PSHE lesson.
- Teachers access Project Evolve to ensure all aspects of Online Safety are covered within the Computing / PSHE Curriculum.
- 'Safer Internet Day' activates that focus on Online Safety during the National Online Safety Awareness Week.

- As part of the Online Safety training children are made aware of the impact of cyberbullying and how to seek help if they are affected by these issues, e.g. talking to a trusted adult in school or parent/carer.

- As part of their Online Safety training and PSHE, children develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of technology both within and outside school. AUP appropriate to the Key Stage to be displayed in all classes and AUP to be signed by all pupils.

- Children are reminded of safe Internet use through corridor and classroom displays.

- Children to only use search engines in school which are appropriate for their learning.

E-mail

The school

- Provides staff with an email account for their professional use *email* and makes clear personal email should be through a separate account;

- Does not publish personal e-mail addresses of pupils or staff on the school website.

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

- Will ensure that email accounts are maintained and up to date

- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils:

- Pupils are taught about the safety and etiquette of using e-mail both in school and at home.

- Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;

- That an e-mail is a form of publishing where the message should be clear, short and concise;
- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
- To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;

  That they should think carefully before sending any attachments;
- Embedding adverts is not allowed;
- That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;

- Not to respond to malicious or threatening messages;
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- Not to arrange to meet anyone they meet through online contact without having discussed with a trusted adult and taking a responsible adult with them;
- That forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use the LA e-mail systems on the school system
- Staff only use LA e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked Never use email to transfer staff or pupil personal data.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
- The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- The sending of chain letters is not permitted;
- Embedding adverts is not allowed;

- All staff sign our LA code of conduct and the use of social network sites and social media policies to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Head teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers:
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Website

- Uploading of information on the schools' website is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's website will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the shared drive.

Social networking

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 30 days*), without permission except where disclosed to the Police as part of a criminal investigation. See separate policy.

Equipment and Digital Content

Personal mobile phones and mobile devices

- Staff members may use their phones during school break times. Phones must not be taken into classroom. They should be left in the staff room. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to

scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- All pupil's mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

Students' use of personal devices

- No students should bring his or her mobile phone or personally-owned device into school. If a student has approval to bring a mobile for a particular reason it must be handed into the office for the school day.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be kept in secure locations as outlined in the staff handbook. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Trips / events away from school

For school trips/events away from school, teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.