

Holy Trinity Church of England (VA) Primary School



Believe • Achieve • Inspire •

Online Safety Policy

SCHOOL VISION

Our vision is for our pupils to flourish in an inclusive, inspirational place of learning where we are happy, respectful, kind and safe.

At Holy Trinity Church of England Primary School our Christian vision shapes all we do.

*"I know that there is nothing better for people than to be happy and to do good while they live."
Ecclesiastes 3:12.*

- we facilitate opportunities so every child can flourish in a place where they feel **safe, happy and confident**.
- staff **well-being** and professional development is valued and supported in order to fulfil their roles, **inspire** others and experience personal **fulfilment**.
- the school provides facilities that enables our pupils to reach their potential in an **optimum learning environment**.
- the **school plays a central role within our community** and enjoys strong **links with the church, local companies and other schools**.
- we create a culture of vigilance to **safeguard** all children.

COMPUTING VISION

At Holy Trinity CE Primary School our vision for computing is that technology is an everyday tool where children can independently and safely apply their computing skills across the curriculum to enhance learning.

INTERNET USE

The purpose of the internet and the school website in school is to raise standards, to promote achievement, to support the professional work of staff and to enhance the school's management information systems.

- Internet access is an entitlement and a necessary tool for staff and pupils.
- The school has a duty to provide children with safe, quality internet access as part of their learning experience.
- Pupils should where possible have equal access to computing within school.
- The school internet access will be designed for pupil use and will include robust filtering appropriate to the age of the pupils.
- Internet access triggers daily monitoring reports sent to the DSLs to enable quick intervention of inappropriate or unsafe searches.
- Pupils will be taught how to use the internet and websites safely and staff will guide pupils in online activities.
- Internet access will be planned to enrich and extend learning activities.
- The school website provides a safe secure environment to access appropriate websites that can support and extend learning.

Provision is made for those pupils who do not have access to the internet or a computer at home through discussion with parents.

CURRICULUM

At Holy Trinity, we use Purple Mash to deliver the Computing Curriculum. We also use 2BeSafe - Being Safe in a Digital World aligned with the [Education for a Connected World](#) framework. The following strands will be the focus in each year group:



Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and media influence in propagating stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.



Online relationships

This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.



Online reputation

This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.



Online bullying

This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.



Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to our physical safety as well as online safety. It also covers learning relevant to ethical publishing.



Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle e.g. mood, sleep, body health and relationships. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.



Privacy and security

This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.



Copyright and ownership

This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

***'I know that there is nothing better for people than to be happy and to do good while they live.'* Ecclesiastes 3:12**

Parent guides for each of these strands of the 2BeSafe curriculum can be found on our website [here](#).

FILTERING & MONITORING

- Our internet is filtered by Sophos Web filter
- If staff or pupils discover unsuitable sites, the URL (address) should be reported to the subject leader and Headteacher who will inform the local authority and the broadband provider. IT support at TSI will be informed to add the URL to the filtered list.
- Where possible staff should view websites before using with the children.
- Pupils will be taught about Internet Safety through the computing curriculum, PSHE and RHSE sessions, planned assemblies and follow up work in the classroom. *(See Appendix 3 and 4)*

CHILD PROTECTION / DESIGNATED SAFEGUARDING LEADS

All DSLs are trained in internet safety issues and are aware of the potential for serious child protection / safeguarding 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
- mobile phone sexting – sharing of inappropriate images

STAFF EMAIL

- Staff and Governors are supplied with a school email account. All school communications will be sent through the school email system and not through personal email accounts.

CONTENT OF WEBSITE

- The point of contact on the website is the school address, email and telephone. Staff and pupils home information will not be published.
- Photographs of pupils on the website will only be included where parents have given permission. Where photographs are used, they will not include names of individual pupils.
- Class pages on the school website will provide curriculum/timetable information for parents along with links to useful websites.

BLOG

- Older pupils will be encouraged to add comments to the school's secure blog as directed by their class teacher on the school's website. Comments should always be moderated and approved by staff. Any unsuitable comment should be discussed with the pupil. Comments that are offensive should be logged in the office and access may be removed.

ACCESS

- The school will keep a record of all staff who have access to the school email or website. The record will be kept up to date so that if a member of staff or pupil leave access is withdrawn. The subject leader will keep this record.
- At Key Stage 1, access to the internet will be by adult demonstration and supervision at all times.

***'I know that there is nothing better for people than to be happy and to do good while they live.'* Ecclesiastes 3:12**

- Methods to identify, assess and minimise risk will be reviewed regularly.
- The Headteacher and subject leader will ensure that the Online Safety Policy is implemented.
- Online Safety guidance will be sent out to parents through the [school website](#), newsletter and information events.
- A partnership approach with parents will be encouraged. This could include demonstrations, published materials and online safety presentations held for parents. Parents will sign Online and Computing Consent Form when their child starts school. (Appendix 1).

REPORTING ONLINE SAFEGUARDING CONCERNS

Staff will use CPOMS to report any concerns they have about a child's online conduct. This may include reports of online behaviours from outside school.

SEND AND ONLINE SAFETY

Pupils with SEND or who are particularly vulnerable will be supported with online access in school. Activities may be adapted to meet their needs. Staff will be vigilant when hearing any reports of concerns from parents or pupils and report on CPOMS if needed.

CYBER BULLYING, ONLINE GROOMING AND RADICALISATION

Pupils will be taught how to stay safe online in and out of school. Any reports of cyber bullying will be dealt with following the Anti-Bullying Policy, and reported on CPOMS. Any reports of grooming or suspicions of grooming will be dealt with following the Safeguarding and Child Protection Policy and reported on CPOMS. Any reports or suspicions of radicalisation will be dealt with following our Prevent Policy and reported on CPOMS.

SECURITY

- All staff must be aware of and adhere to the Acceptable Use Policy and Online Safety Policy.
- Policies will be agreed by Governors and available on the school's website.
- The school computing systems are reviewed regularly with regard to security supported by TSI. Recommendations are acted on by the subject leader and Headteacher.
- The technician will update the server so that only current staff and pupils have access to the school system.

TRAINING

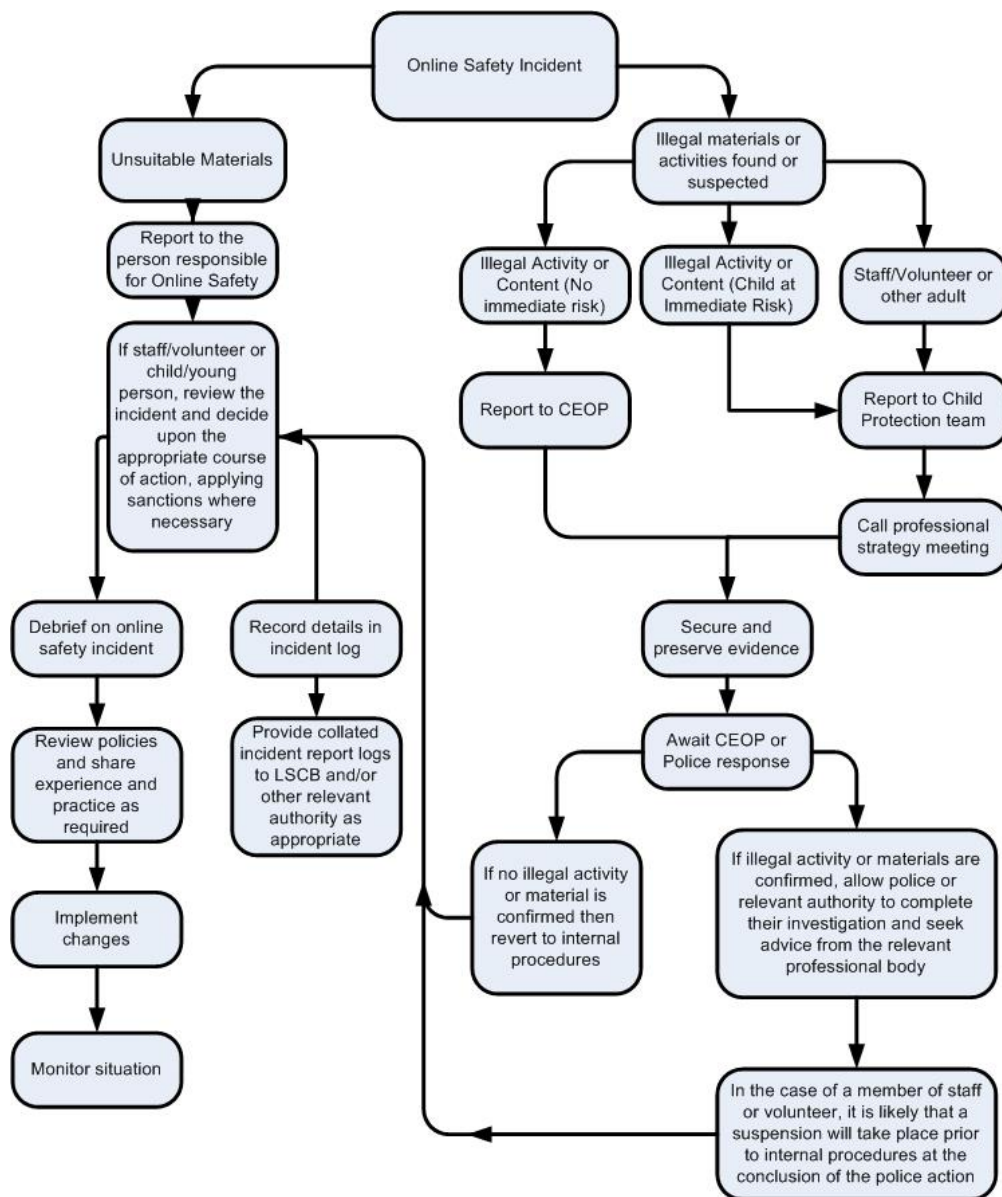
A planned programme of formal online safety training will be made available to staff and nominated governors. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.

The Online Safety Coordinator (Computing subject leader) will provide advice / guidance / training to individuals as required.

ILLEGAL INCIDENTS

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police. See Safeguarding and Child Protection Policy.



OTHER INCIDENTS

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

IN THE EVENT OF SUSPICION, ALL STEPS IN THIS PROCEDURE SHOULD BE FOLLOWED:

- Have more than one senior member of staff / governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

'I know that there is nothing better for people than to be happy and to do good while they live.' Ecclesiastes 3:12

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the report form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant)
 - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - incidents of the require reporting to Prevent
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

This policy was adopted by Holy Trinity CE Primary School and agreed by the Standards, Achievements and Curriculum Committee and ratified by the Full Governing Board.

Approved by.....on behalf of the School Governing Board.

Signature:.....

Date:.....

Links to useful documents:

[DFE Teaching online safety in school](#)

[DFE Relationships Education, Relationships and Sex Education \(RSE\) and Health Education 2025](#)

[DFE Sexting Schools and Colleges](#)

[UKCCIS: Education for a Connected World](#)

Related policies:

Acceptable Use Policies

Safeguarding and Child Protection Policy

Staff Code of Conduct Policy

Mobile Phone Policy

GDPR Data Protection Policy

Prevent Policy

Anti-Bullying Policy

Behaviour Policy

Remote Learning Policy

RHSE Policy

Staff Code of Conduct

Online & Computing Consent Form

Pupil's Name:	
---------------	--

As the Parent or legal guardian of the above pupil, I give permission for my child to have access to the internet and computing facilities at Holy Trinity CE Primary School.

I'm aware of the Online Safety Policy of the school (available on the school's website).

I understand the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate content. These steps include using a filtered internet service, employing effective teaching practice and delivering Online Safety sessions regularly equipping pupils with knowledge of how to stay safe and report concerns.

I will support the school by promoting safe use of the internet and technology at home and will inform the school if I have any concerns over my child's online safety.

Please tick below as appropriate:

I agree that my child will follow Holy Trinity's rules for responsible use of the internet and computing as outlined in our school's Online Safety Policy.	
I do not agree that my child will follow Holy Trinity's rules for responsible use of the internet and computing as outlined in our school's Online Safety Policy.	

Signed:	
Date:	