Holy Trinity Primary School Internet and Online Safety Policy

Introduction

The purpose of this policy is to:

- establish the ground rules we have in school for using the Internet and electronic equipment
- describe how these fit into the wider context of our discipline and PSHE policies
- demonstrate the methods used to protect the children from unsuitable material

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

At Holy Trinity we feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents. Parents are sent an explanatory letter and the rules which form our Internet Access Agreement. This can be seen as an extension to the Home School Agreement.

Why the Internet and emergent technology are important

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

How the Internet benefits education

We consider the Internet to be vital for educational development.
Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and best curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LEA and Government agencies;
- improved communications between the home and school.

How the Internet will enhance teaching and learning

At school internet access is designed for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Internet access is planned to enrich and extend learning activities.
Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.
Our school uses MyMaths, in which children can carry out their maths homework online. Our school has also bought into Purple Mash which is an online educational resource and this is used at school. We also use IDL as a tool to improve spelling and reading.

Evaluating Internet content

Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
Where training is necessary it will be made available to staff in the evaluation of Web materials and methods of developing students' critical attitudes. As far as possible, Internet searches and website content should be checked by an adult prior to the children using the Internet, especially when search terms may be ambiguous.
If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider within the LEA. This is done by reporting any incident to the Computing Subject Leader and Headteacher, who will record the Incident in the Internet Incident Log.

Managing website content

Holy Trinity Primary School has its own website. Staff or pupils' home information will not be published on the website. The website will not mention any pupils by their full name and photographs will be selected carefully so that individual pupils are not named. Holy Trinity Primary School also has its own twitter account. This contains tweets and photographs from whole school events and class work. The aim of our twitter account is to keep parents and carers up to date about what is happening in school. Class One have a blog that contains photographs and information about what the children have been doing in class. The same rules apply to the blog and twitter as the school website. Written permission from parents or carers will be obtained through the Holy Trinity Internet Access Agreement before photographs of pupils are published on the school website/blog.
The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate.
The copyright of all material that appears on the website must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
It is the responsibility of year group teachers to appropriately update their individual sections of the school website.

Managing emerging Internet uses

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Authorising Internet access

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.
At Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
In Key Stage Two, children will be expected to carry out focussed searches using the Internet and any work done on the Internet should be done with an adult present.
Access to Purple Mash is given to all pupils from Reception to Year 6. My Maths is available to KS1 and KS2. IDL is used throughout the school for individual children to enhance their learning and progress in spelling and reading.

Assessing risks

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Lancashire Education Authority can accept liability for the material accessed, or any consequences of Internet access.
Methods to identify, assess and minimise risks will be reviewed regularly.

The Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored. The following table outlines some of the potential risks:

Area of risk	Examples of risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising Privacy of information (phishing, identity fraud) Invasive software (e.g. virus, trojan, spyware) Online gambling Premium rate sites
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate / bias materials Inappropriate materials Copyright and plagiarism User generated content (e.g. YouTube,)
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact inappropriate emails / blogs / instant messaging Encouraging inappropriate contact

Internet filtering

The school will work in partnership with parents, Lancashire LEA, and the DfE guidelines to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover unsuitable sites, the URL (address) and content must be immediately reported to the Internet Service Provider via the Computing co-ordinator. Any material that the school believes is illegal must be referred to the Local Education Authority.
All internet devices belonging to school use Internet Content Filtering provided by Lancashire LEA.
IMPORTANT NOTE: It should be noted that the main aim of content filtering is to MINIMISE THE RISK OF USERS ACCESSING INAPPROPRIATE MATERIAL ON THE INTERNET. Whilst the content filtering provision will significantly contribute towards this, it should NOT be viewed as a complete solution that will block all inappropriate material and therefore should be underpinned with good practice at home and at school.

Lancashire LEA operate a devolved filtering system where schools can unblock certain sites at a local level without having to refer the request to Lancashire. This can be useful when sites with good educational content are blocked erroneously. Unblocking a site can only be done with the Headteacher's specific permission. It must also be noted that once a site is unblocked it is unblocked

across the entire school, not just on the machine that is being used. A record of staff who unblock websites is kept by the filtering software and it is imperative that the address is blocked once again after it has been used. It is envisaged that this feature of the filtering system will be used sparingly. If staff want to request the unblocking of a website they will need to ask the Computing Leader or Headteacher.

Introducing the Internet policy

Rules for Internet access will be posted near all computer systems.
Pupils will be informed that Internet use will be monitored.
Instruction in responsible and safe use should precede Internet access in each year group. This policy will be made available to parents via the Holy Trinity website.

Staff consultation

All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance will be explained.
Staff should be aware that Internet traffic can be monitored and traced. Discretion and professional conduct is essential.
The monitoring of Internet use is a sensitive matter, and staff who operate monitoring procedures will be supervised by senior management.
Staff development in the safe and responsible use of the Internet will be provided as required.
Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

Staff must never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) .They are licensed to investigate – schools are not!

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred.

More details on these categories can be found on the IWF website (www.iwf.org.uk)

Inappropriate use

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. The following table outlines possible incidents alongside procedures and sanctions:

<table>
<tr><th>Incident</th><th>Procedures and sanctions</th></tr>
<tr><td>Accidental access to inappropriate materials.</td><td>Minimise the webpage.
Children to tell a trusted adult in the lesson.
Report the incident to the Computing Leader who will record it in the incident log.
Report to LGFL filtering services if necessary.
Inform parents / carers.</td></tr>
<tr><td>Using other people's logins and passwords maliciously.
Deliberately searching for inappropriate materials.
Bringing inappropriate electronic files from home.
Using chats and forums in an inappropriate way.</td><td>Inform Senior Leadership Team and Computing Leader.
Record the details in the incident log.
Inform parents / carers.
Consider additional eSafety awareness raising lessons.
More serious or persistent offences may result in disciplinary action in line with the Behaviour Policy.</td></tr>
</table>

Infrastructure and Technology

Children's access

Children should always be supervised when accessing school equipment and online material. Children have year group logons to gain access to the school network. The staff server cannot be accessed by pupils.

Passwords

Holy Trinity Online Safety rules remind children that passwords should be kept secret.
The school ICT technicians Mr. John Kavanagh / Mr. Patrick Costelloe hold the administrator password.

Software / Hardware

Holy Trinity has legal ownership and licenses for all software.

Software installation is controlled by Mr. Patrick Costelloe.

Managing the network and technical support

All servers, wireless systems and cabling are located away from children who cannot access them. All wireless devices are security enabled.
I-pads have passwords to access the app store. IT technicians have the passwords for this.
All staff are responsible for the security of the network. Any security risks should be reported immediately to Mr. Patrick Costelloe. All laptops are updated with Sophos virus protection through the school server. Staff and children have defined access rights to the network which is managed by Mr. Patrick Costelloe. Any breaches of network security should be reported to Mrs. Carlile. Mrs. Lyle and Mrs Carlile liaise with Mr. Costelloe regarding the school network.
The school has the 'Light-Speed' filtering system as recommended by the local authority. This filter is managed by Mr. Costelloe who alerts the Headteacher to any inappropriate content that has been discovered. Youtube is 'blocked' by the 'Light-Speed' filter at the Headteacher's request but this can be over-ridden by the teachers for a 10 minute period only if they wish to show an educational video.

Dealing with incidents

All online safety incidents should be entered into the incident log which is held in the Headteacher's room. Any incidents should also be mentioned in the weekly wellbeing meeting especially if they could be deemed as bullying or racist. Where appropriate the Headteacher may decide to share information relating to an online safety incident if it may warn other parents / children to be vigilant to an aspect of online safety.

Use of digital media cameras and recording devices

Photographs and videos of children and adults may be considered as personal data in terms of the Data Protection Act 1998 and General Data Protection Regulations.

Consent and Purpose

School collects and stores written consent from parents for photographs of their children to be taken or used. Parents are made aware of how photographs could be used e.g. on Facebook, Twitter, school website, in brochures or displays. Permissions are obtained when a child starts school; however parents may request permission for removal whenever they feel is appropriate, a 'withdrawn permission' form is available from the School Office. Any pupil who does not have consent for photographs must not be used for press purposes.

Taking Photographs / Video

- Any member of staff wishing to take images of children must be approved by the Headteacher.
- Photographs on a school camera or class Ipad must be immediately uploaded to the

staff server and deleted from the device.

- No pupils should be continually favoured in images.
- Photographs taken will not be embarrassing, or show any pupils in distress or situations which could be misinterpreted.
- Close up shots should be avoided as these may be considered intrusive. Shots should preferably include a background context and show children in group situations.

Parents Taking Photographs / Video

Under the Data Protection Act 1998 and General Data Protection Regulations, parents are entitled to take photographs of their own children under the provision that the images are for their own use. Including other children or other purpose could constitute a potential breach of Data Protection legislation.

• Parents are advised that they should only photograph their own children at events.

• Parents are reminded at school events that publishing images which include other children than their own or adults on social networking sites are not acceptable, unless permission has been obtained from the subjects.

• Parents will be reminded to be considerate of other audience members when taking photographs at events.

Storage of Photographs / videos

• Any photographs taken will be uploaded to the school server and added to the staff section which children can no access. • Images on cameras / i-pads must be deleted once added to the server. • Staff must not store personal images on school equipment. • Class teachers have responsibility to delete images from Ipads and this will be monitored by Mrs Lyle.

Publication of Photographs / Videos

• Consent is needed from parents for publication of children's images e.g. on the school website.

• Names or other personal information will not accompany published images.

• Staff will not publish school photographs on personal social networking sites.

The media, 3rd Parties and Copyright

All 3rd parties will be supervised at all times whilst in school and must comply with the Data Protection requirement in terms of taking, storing and transferring images.

CCTV, Video Conferencing, VOIP and Webcams

At Holy Trinity, there are 12 external CCTV cameras which cover the carpark, paths around the school building and the playground. (See additional CCTV policy) Should video conferencing be used to enhance the curriculum, parental permission will be sought beforehand.

Communication Technologies

Holy Trinity uses a variety of communication technologies and is aware of the benefits associated with their use. Should new technologies be introduced this policy will be updated accordingly.

Email

- All staff should use their Holy Trinity email account to communicate on school matters.
- All users are informed that email communications may be monitored at any time in accordance with the acceptable use policy.
- Staff are informed that any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature should be reported to Mrs. Lyle.
- As part of learning, email may be used by pupils. If an instance occurs where the use of email will enhance learning then the class teacher will inform Mrs. Lyle who will set up accounts for the children. Any such accounts will be monitored by the class teacher.
- Pupils must not arrange a meeting through email communication.
- The forwarding of chain letters is not permitted.
- Education about email safety will be covered in the online safety provision for parents, staff and pupils. The use of e-mail is in the Key Stage Two Scheme of Work for Computing. Children in Key Stage Two have access to 2email (via Purple Mash) and can use the 'Maily' app on the IPAD's for emails (safe messaging for young children). The school's Rules for Responsible Internet Use include the use of e-mail. Pupils must immediately tell a teacher if they receive an offensive e-mail. Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.

Social networking

Holy Trinity uses Twitter and a blog social media sites as tool to communicate with parents.

- Teachers have control of the school Twitter account and they are all responsible for its content.

- Photographs will only be added to the sites if internet permission has been agreed by parents / carers.

- No child will be 'tagged' or named by school.

- Children will not be friended by school as the pages / sites are designed to share news with parents, not children.

- Parents are regularly reminded that Twitter is a positive line of communication between home and school and that any negative comments or complaints parents may wish to make should be directed to the Headteacher or class teacher directly rather than be shared via social media.

• Staff will be reminded that if they 'like' or 'follow' Holy Trinity that they can then be seen by parents and their profiles should have the highest security settings so that they do not attract unwanted attention.

• Any staff using social media should ensure that content posted online should not:

- Bring the school into disrepute
- Lead to valid parental complaints
- Be deemed as derogatory towards the school and/or its employees
- Be deemed as derogatory towards pupils and/or parent and carers
- Bring into question their appropriateness to work with children and young people

Instant messaging

Instant messaging such as texting, Skype, FaceTime and popular communication tools with both adults and children. They can provide an opportunity to communicate in 'real time' using text, sound and video.

• Staff should not share their mobile number with parents

• Staff should not use school equipment to communicate with personal contacts. (e.g. using a school Ipad to FaceTime their friend.)

• If using any of these types of messaging as a learning tool to connect with people outside school, the Headteacher should be consulted beforehand.

Mobile Phones

Staff may use their mobile phone for personal reasons in school but this should never happen during teaching time. During the school day, mobile phones should be switched to 'silent' so that they do not disrupt learning and should be left in the Staffroom during teaching time. No mobile phones must be used in toilets or where children may be changing. If staff believe there is suspicious use of mobile phones they must inform Mrs. Lyle or Mrs. Carlile immediately. School does not accept responsibility for any breakages to mobile devices. Staff are responsible for their own personal devices.

Children are not allowed mobile phones in school unless there is an exceptional reason. In this case, they should be handed into the office and a consent form can be filled in. School accept no responsibility for the mobile phones.

Video Conferencing

Holy Trinity School has access to video conferencing equipment in class 4 . Children and staff may be familiar with video conferencing through widely used software such as Skype. There are a few points to consider when using video conferencing in school:

- The children must have permission to do video conferencing. There is a section on the internet agreement letter and a full list is given to each teacher.
- It is important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.
- Approval by the Headteacher must be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to stop or hang up the call.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

How will ICT system security be maintained?

The school ICT systems will be reviewed regularly with regard to security. Virus protection will be installed and updated regularly by the ICT technician.

Handling Internet related complaints

Responsibility for handling incidents will be delegated to a senior member of staff. If inappropriate content is accessed, the incident must be referred to the Computing Leader who will then inform the Headteacher. Any complaint about staff misuse must be referred to the Headteacher. Pupils and parents will be informed of the complaints procedure. Parents and pupils will need to work in partnership with staff to resolve any issues that may arise. Any deliberate misuse of the internet may result in withdrawal of access.

Involving parents

Parents' attention will be drawn to the School Internet Policy in newsletters and on the school website. Internet issues will be handled sensitively to inform parents without undue alarm.
A partnership approach with parents is encouraged. This includes demonstrations, practical sessions and suggestions for safe Internet use at home.

Updating the policy

Our School Internet Policy has been written by the school, building on NGfL policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

Updated by: Mrs Carole Carlile (Computing Subject Leader)
Date: September 2020
To be reviewed: September 2022