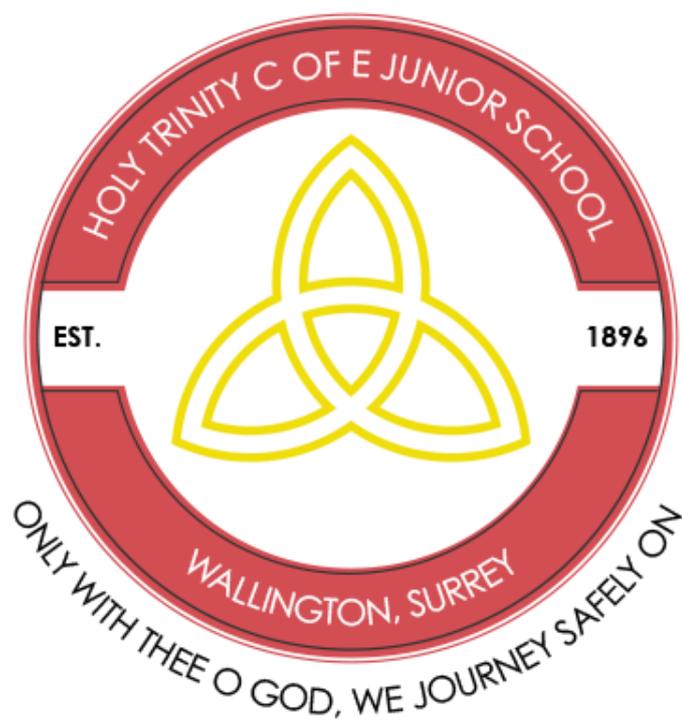


Holy Trinity CE Junior School



Policy for:

E-Safety Policy

Written by:

Mrs Robins

Date Reviewed:

June 2018

Next Review Date:

Summer 2019

Policy

Holy Trinity CofE Junior School

e-Safety Policy

Principles

The Internet is an essential part of modern life. Internet use in school can raise educational standards, promote student achievement, support the professional work of staff and enhance the school's management information and administration systems.

The school therefore has a duty to provide students with quality access to the internet and other modern technologies as part of their learning experience, and ensure they can use the Internet and related communications technologies appropriately and safely.

Our e-safety policy covers all members of the school community, including the Headteacher, all members of staff, pupils, visitors and volunteers. Compliance with the policy ensures that everyone knows and understands their responsibilities and can act upon them.

Aims

The purpose of Internet and digital technology 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 systems.

Practice – in general

Internet access in the school is provided via a broadband link through the LGFL intranet. Filtering appropriate to the age of the pupils is provided as part of this link. The School blocks/filters access to social networking sites and newsgroups unless a specific use is approved for a specific lesson; Youtube is accessible by staff and can be used, where appropriate, to display material in lessons. An agreement for the provision of a suitable virus protection system has been implemented through Cygnet, who monitors and service the school network. This virus protection system is installed on all devices in school and automatically updates regularly. Portable media may not be brought into school without specific permission and a virus check. Pupil access to the Internet will be by adult demonstration or directly **supervised** access to specific, approved on-line materials. Instruction in responsible and safe use by pupils is a core element of the Computing scheme of work.

On entry to school parents and children agree to follow our rules by signing an acceptable use policy. In accordance to GDPR we also seek permission from parents about publishing children's images online (school website).

Children in Year 6 are permitted to bring mobile phones to school [please see Mobile Phone policy]

Practice – for pupils E-safety will be delivered through: Computing and other lessons; assemblies led by staff; workshops led by staff or other LA approved trainers. The curriculum will teach pupils how to stay safe, protect themselves from harm and how to take responsibility for their own and others' safety. As part of the curriculum, pupils will be made aware of the guidelines for the acceptable use of the Internet both in school and in the wider world.

Curriculum activities that involve the use of the Internet for gathering information and resources will develop pupil skills in locating and evaluating materials and will be given clear objectives. Pupils will be taught how to validate materials they read before accepting their accuracy. Where materials gathered from the Internet are used by pupils in their own work, they will be taught to acknowledge the source of information used.

Practice - Staff

As part of the induction policy, all members of staff including teachers, teaching assistants and support staff, will be provided with access to a copy of the school e-safety policy. All staff also signs, and agree to adhere to, a copy of the Staff Acceptable Use Policy (appendix 3) before using any Internet resource in school. Staff will be made aware that Internet traffic can be monitored and traced to the individual user and professional conduct is essential. All e-mail communications sent by members of staff that relate to the school will be through authorised, LGFL StaffMail accounts. The use of online chat rooms and instant messaging services is blocked by the intranet filtering. Staff must not store images of pupils or pupil personal data on personal devices. Staff should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Parent awareness

The school runs a planned programme of advice, guidance and training for parents, including: Acceptable Use Agreements to ensure that principles of e-safe behaviour are made clear; information leaflets; e-safety updates in school newsletters; e-safety guidance clearly signposted, and referred to, on the school web site including national support sites; seminars/ practical sessions held at school.

Responding to incidents of misuse:

It is hoped that all members of the school community will use ICT responsibly and follow this policy. From time to time, as in all aspects of school life, however, pupils make poor judgements with respect to electronic communications. These are followed up in line with Behaviour and Anti-bullying Policies, Staff Code of Conduct, Child Protection Policy or Procedures. Concerns will sensitively be raised with parents. Where necessary, sanctions may be issued and or the police informed. Access to the internet in school may be withdrawn. Should it become necessary to prohibit the use of internet resources for a pupil then parents or carers will be involved so that a partnership approach can be used to resolve any issues. This could include practical sessions and suggestions for safe Internet use at home.

Any illegal activity will be reported to the local police and, for staff, the LADO (Local Authority Designated Officer) as necessary.

The school follows the DfE search and confiscation guidance and Prevent guidance

Monitoring & Evaluation

This policy will be monitored by the teacher responsible for ICT and the Designated Officer for Child Protection. E-safety incidents will be monitored on the safety incident log (appendix 4) and reported to governors. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out, as necessary, before use in school is allowed. The policy will be monitored by Governors via the pupils and curriculum committee.

Appendix I



Parents' Acceptable Use Policy



Internet and ICT:

As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter / son access to:

the Internet at school

ICT facilities and equipment at the school.

As the parent or legal guardian of the pupil(s) named below I grant permission for the school to take photos of my child to use within the building.(eg: displays around the school to celebrate success such as timestable rock stars; photos to display school council; photos of children at work to be printed and stuck into their work books.)

I understand that the school provides the most stringent filtering and Firewall applications in order to protect my child whilst at school, provided by Cygnet.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

Acceptable Use

I know my son/daughter will receive e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand I can take photos/ videos of my child during school assemblies/ shows and that to protect everyone's privacy, and in some cases safety, I **must not** publish these images online – including social media.

I understand that live streaming, whether public or private cannot be permitted. I will not use any streaming platforms or 'live' features (e.g. Facebook Live) to stream events/circumstances as they occur. I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

I know that my son / daughter will sign an Acceptable Use Agreement. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I will work with the school in endorsing the acceptable use policy by being a good role model in my own online practice.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I know that if I have serious concerns about my child's online safety I can report this to Child Exploitation and Online Protection Command (CEOP).

My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ___/___/___



Appendix 2

Acceptable Use Policy Agreement – Children

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may lose access to the school network / internet, my parents will be contacted and the behaviour policy will be adhered to. In the event of illegal activities involvement the police may be involved.

Name

Signed:

Date:



Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, network resources, learning software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will not engage in any online activity that may compromise my professional responsibilities. Including:
 - No reference should be made in social media to students / pupils, parents / carers or school staff
 - Not engaging in online discussion on personal matters relating to members of the school community
 - Not attributing personal opinions to the school /academy or local authority
 - Ensuring security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- I will only use the approved email system(s) for any school business.
This is currently: [LGfL StaffMail]
- I will not browse, download or send material that could be considered offensive to colleagues. (see equalities policy)
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- I will follow the school's policy on use of mobile phones
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- Staff that have a teaching role only: I will support the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the e-safety Coordinator, the Designated Child Protection Officer or Head teacher.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

Appendix 4- E-safety incident log

Reporting Log						
Group:						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		