HOLY TRINITY PEWLEY DOWN

A Federation of Holy Trinity Junior & Pewley Down Infant Schools, Guildford

E-Safety and ICT POLICY

Introduction

HTPD believes that the use of information and communication technologies in schools brings great benefits. Recognising the e-safety issues and planning accordingly will help to ensure appropriate, effective and safe use of electronic communications. At HTPD**,** we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Childnet International equates the internet to bringing a city into your living room: there are exciting places for children to go and enjoy, but also lots of places where you would not want children to go unsupervised. The main dangers for children are:

- Potential contact from someone online who may wish to harm them.
- Children must re-learn the 'stranger-danger' rule in a new context and never give out personal details or meet alone with anyone they have contacted via the internet.
- Inappropriate content that children may be viewing. It is important to agree the ground rules about where the children can go and how they behave.
- Excessive commercialism and advertising which invades children's privacy. Encourage children not to fill in forms which ask for lots of personal details.

Why use the internet?

- 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 functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for pupils 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 pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

There is a very clear link between the E-Safety and ICT Policy and other existing school policies such as (but not limited to) Behaviour and Anti-Bullying.

It is essential that all staff and pupils are aware of what is considered acceptable conduct and staff subsequently recognise their professional responsibilities when using ICT equipment and systems.

The School will:

- Provide the best possible equipment and service affordable to all its staff and pupils;
- Ensure that users are able to operate in a safe and secure environment;
- Educate staff and pupils on new technologies and the risks associated with them;
- Provide training/information with regard to the responsible use of ICT which will, in turn, promote e-safety.

E-safety refers to the safe and appropriate use of the internet and any associated gateways including social media whilst ICT refers to the physical equipment being used.

In order to make clear the purpose of the E-Safety and ICT Policy, it is underpinned by 2 key documents that ensure all staff and pupils accept responsibility for their actions as below:

1. Staff Acceptable Use Policy **(Appendix 1)**
2. Safe use of the internet – a guide for HTPD pupils **(Appendix 2)**

All staff will be requested to sign the Staff Acceptable Use Policy (Appendix 1) and are expected to adhere to the policy. All pupils will be made aware of what safe and acceptable use of ICT equipment and the internet as part of the curriculum.

Safety concerns and advice

- HTPD will appoint an e-Safety Coordinator. This may be the Designated Child Protection Co-ordinator as the roles overlap.
- Our e-Safety and ICT Policy has been written by the school, building on government guidance. It has been agreed by the senior management and approved by governors.
- Pupils should be taught to be critically aware of the materials they read and be shown how to validate information before accepting its accuracy.
- The security of the school information systems will be reviewed regularly.
- Whole-class or group e-mail addresses should be used rather than pupil email addresses.
- The contact details given on the school website should be the school address, e-mail and telephone number. Pupils' personal information must not be published.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. Examples include real names, addresses, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests, clubs, etc.
- Blocking strategies operated by Surrey will prevent access to a list of unsuitable sites.
- Pupils will not be able to access social networking sites which the school will filter access to.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. HTPD cannot accept liability for material accessed, or any consequences resulting from Internet use.
- Any complaints of internet misuse will be dealt with by a senior member of staff.
- E-safety rules will be posted in classrooms and near PC's in the schools.
- Pupils will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.

Response Protocol to reported ICT Incidents

It is important that any report of inappropriate use of ICT equipment and associated software is able to be reported without fear of repercussions and hence any reports made will initially be treated in the strictest of confidence.

Review

The Governing Body of HTPD first adopted this policy in 2012. It will be reviewed bi-annually.

Date last reviewed: **December 2017**

Date for next review: **December 2019**

Signed:

Mark Sharman
Governor of Holy Trinity Junior & Pewley Down Infant Schools
ECM

Appendix 1

Staff Acceptable Use Policy

Devices

- Staff will take responsibility for all activity that takes place whilst using a device logged on to the server.
- Any ICT problems/issues should be reported to the IT Manager or Business Manager
- ICT devices should not be used for anything illegal
- The School reserves the right to monitor all staff devices and associated usage taking place on the school site and also any usage of school owned devices in any location in the world
- No software may be in installed on any school owned device without the consent of the ICT Manager.
- Staff will take responsibility for all activity that takes place under their own login on their device (whether owned by the school or personally) .
- Passwords are to be kept confidential and changed when requested to do so.
- Individually issued devices must not be used by non-school employees (see also the Staff Ipad Loan Agreement if applicable).
- Devices may temporarily be left in a locked vehicle if locked away in the boot and out of sight. They should not be stored or left in a vehicle overnight.
- Staff must not attempt to disable or remove monitoring software on any machine.
- Staff must not attempt to disable or remove the virus checker software on any machine.

Storage/Printing

- Staff must be mindful of available space on the server and email storage and regularly clear out old and unwanted files.
- Printouts should be in black and white (where possible) and kept to a minimum. Multiple copies (more than 30) should be produced via the ‘fast photocopier’ where applicable.

Internet & Email

- Staff must assume responsibility for any sites visited, files downloaded, content viewed or emails received/sent using or on a school device/network.
- Staff must not attempt to bypass the schools filtering system by attempting to access proxy sites.
- The use of email/internet for the following reasons is forbidden:
  - betting and/or gambling
  - personal financial gain
  - advertising purposes
  - political purposes
  - viewing / downloading of racist, pornographic, sexist, obscene or any other unsuitable material
  - posting of anonymous messages
  - sending libellous, slanderous, threatening or abusive messages
  - any illegal activities
- The copyright and intellectual property rights of all content viewed / downloaded must be respected.
- Staff should beware of emails and/or attachments from unknown sources. If in doubt, delete immediately. Do not open any suspicious message(s).

- The School accepts no liability for any personal financial transactions which are made across the internet/email
- Where inappropriate sites are accessed by accident the IT Manager should be informed immediately.
- Staff should note that emails can be as legally binding as a written letter.
- Non-required emails and attachments should be deleted once read.
- Nothing should be sent via email that could tarnish the School's name or expose it to legal action.
- The contents of any sent email must not infringe copyright.

E-Safety

- Personal Data
  - No personal data, including information relating to students, should ever be passed on to an unsecured third party individual or site.
- Social Networking Sites
  - Staff should not be 'friends' with any pupils or ex-pupils who are under the age of 18 when using social networking sites (e.g. Facebook).
- Images
  - Staff may only take images of pupils for official school purposes.
  - Images of pupils (i.e. trips, visits, events, etc.) must only be stored on the school network.
  - Any images captured on personal devices must be moved (e.g. by email) to the server as soon as practicable so that they can be stored securely.
  - Images of pupils should be deleted after the pupil has left.
- Contact Details
  - Staff should be cautious in giving out contact details and should never give their personal email address to a parent or pupil.
- Emailing parents
  - Emails to parents must only be made using school email accounts. Staff should not email pupils directly.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Breach of Staff Acceptable Use Policy

- Any breach of the **Staff Acceptable Use Policy** may be deemed as misconduct and dealt with in accordance with the School's **Disciplinary Policy**.

I understand and agree to abide by the above Staff Acceptable Use Policy

Staff Name (please print).....

Staff Signature.....

Date.....

Appendix 2

Safe use of the internet – a guide for HTPD pupils

This appendix should be adapted by each year group to ensure that it is appropriate to the age group and its needs. A child friendly version should be displayed in each classroom for children to refer to.

Each year group should cover the points mentioned in this Appendix in an age-appropriate manner.

School computers

- Pupils must accept responsibility for all activity that takes place under their own network login.
- Pupils may only use their own network accounts.
- School computers must only be used for school business and must not be used for any illegal, obscene, offensive, profit making or commercial purpose.
- Pupils should be aware that the School is able to monitor all computers, devices and what they are being used for both at school and any usage of school owned devices in any location in the world.
- No software may be in installed on any school owned device.
- Passwords must be kept confidential and changed when requested to do so.
- Pupils must not alter any of the settings on school owned devices.
- Any ICT problems/issues should be reported to the teacher immediately.

Internet & Email

- School internet must only be used for school related work.
- Emails should be sent/received using a school registered account only. Access to hotmail and other internet based email accounts is forbidden.
- The copyright and intellectual property rights of all content viewed / downloaded must be respected.
- Emails and/or attachments from unknown/suspicious sources should not be opened and should be deleted immediately.
- Non-required emails and attachments should be deleted once read.
- Where inappropriate sites are accessed by accident the teacher should be informed immediately.

E-Safety Guidance

- Personal data should never be passed on to anyone.
- Pupils should never agree to meet people they have met on-line.
- Access to social networking/chat room sites is not permitted in school.
- Photos of staff and students must not be labelled and/or copied from the school network.
- Pupils must not pass on anyone else's contact details without permission.