Cam Hopton Church of England Primary School (Voluntary Aided)

E-SAFETY POLICY

Celebrating the achievement of all by living and learning together
‘Jesus offers life in all its fullness’

Document History

Document held at: School, Editor and Secretary to the Governors

Committee Responsible:

Document Version	Date	Author/Editor (ED)	Version Identifier (ddmmyyyy_ED)
Original:	May 2011	ICT Cluster	
Author:	March 2018	Becky Harris	22-03-2018 _BH
Approval:	March 2018	TLS	27-03-2018 _BH
Next review due:	March 2020		

This policy is to be reviewed in line with other related policies and any other documentation from the DfE, Ofsted and Gloucestershire Diocese.

CAM HOPTON CHURCH OF ENGLAND PRIMARY SCHOOL
[Voluntary Aided]

E-SAFETY POLICY

CONTENTS

1.0 Introduction

Cam Hopton Church of England Primary School (CHS) provides pupil access to material on the internet for educational purposes. Pupils may also be taught to send and receive e-mails and to publish articles on the school's website. This policy sets out the rules and procedures which are intended to keep pupils safe with respect to the following on-line hazards: viewing or downloading unsuitable internet content, breaching copyright law, sending out unsuitable material or personal information and being deceived into entering inappropriate relationships with strangers.

The main safeguards employed by the school are: close supervision of pupils whilst using the school's computers, restriction of access to trusted internet resources, and the blocking of resources known or reported to be inappropriate.

However, given the complexity and ever-changing nature of internet and the multitude of linkages between websites and file attachments, etc. it is not possible to give an absolute assurance that unsuitable material will never be accessed by pupils using school computers.

The E-Safety Policy is closely related to the CHS Acceptable Use of IT Policy and the CHS Safeguarding and Child Protection Policy.

2.0 Responsibilities

The School's E-Safety Lead is the Designated Safeguarding Lead (DSL).

The DSL will be supported in this role by the Deputy DSL's, the Computing Lead and the Safeguarding Governor. The policy will be regularly reviewed with all staff.

3.0 Internet Access

- The school has a duty to provide pupils with quality internet access as part of their learning experience.
- The internet is an essential element in 21st century life for education, business and social interaction.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning.
- Safe use of the internet will be taught discretely and alongside internet use for other subjects where appropriate.
- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.
- Pupils will be taught how to evaluate internet content.

- The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught the importance of password privacy.
- Pupils will be taught how to report unpleasant internet content.
- Staff are expected to adhere to the current internet safety guidelines as stated by the South West Grid for learning (SWGfl - www.swgfl.org.uk).
- Pupils will be supervised by teachers or teaching assistants (TA's) whilst accessing the internet. The aim is to provide continuous supervision by a responsible adult. However, it must be recognised that the teaching staff will not, in general, be working with pupils on a one-to-one basis. Also, teaching staff are subject to distractions and interruptions which may divert them, temporarily, from such supervision.
- Pupils will be taught not to follow internet links, open attachments or download files until their supervisor gives permission.
- Teachers and teaching assistants will access only suitable, trusted websites when working with pupils on the internet.
- Any websites found to be unsuitable will be blocked to prevent access from school computers.
- Pupils will be taught never to give out personal details of any kind which may identify them, their friends or their location.

4.0 E-mail

- When available, pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- In-coming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mails from pupils to external bodies are presented and controlled.
- The forwarding of chain letters is not permitted.
- Pupils will be supervised by teachers or teaching assistants (TA's) whilst sending or receiving emails and inserting and opening email attachments**.**

5.0 Published Content and the School Website

- Staff or pupil personal contact information will not be published. The contact details given on-line should be those of the school office (admin@camhopton.gloucs.sch.uk).
- The Office Manager and Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Where possible group photographs will be used rather than full face photos of individual children and will only be shown on the website if parents/carers have signed a consent form.
- Pupils' names will not be used in association with photographs anywhere on the school web site or other on-line space.

- Parents will be clearly informed of the school's stance on image taking and publishing.

- On school premises and outside of public events, photographs and videos of pupils will be taken only by: teachers, teaching assistants (TA's), parents/volunteers/others under the instruction of the HT or by professional photographers contracted to do so by the school. Teachers and TA's are to use off-line cameras and dedicated memory cards/devices/films as far as possible. Should personal equipment be used to record images, they should be downloaded as soon as possible and erased from that device. The school expects teachers and TA's to accept professional responsibility for the use and safe storage/deletion of such images. Images taken which are later found to be in breach of parent/carer consent, should be deleted.

- The ruling above also applies during off-site educational activities, sporting events, church services, etc. However, the school cannot accept responsibility for images of pupils taken by others in public places or off-site premises visited. Both at school and during off-site activities, staff will record and report any persons suspected taking an undue interest in pupils.

- The school does not accept responsibility for photographs and video images taken at the school during public events: assemblies, school plays, fêtes, etc. which may be attended by persons other than pupils' parents, carers and pupils' family members. Attendees at such open events are advised that some parents and carers may object to images being taken of their children.

- In an emergency, such as a child protection matter or an accident, members of staff, pupils, parents and others are encouraged to record the event by any means available, in order to secure evidence that might prove to be important in any subsequent investigation.

6.0 Social Networking and Personal Publishing

- Social networking sites are not permitted for use in school.
- Pupils and parents will be advised that the use of social network spaces outside of school brings a range of dangers for primary aged pupils.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be taught never to give out personal details of any kind which may identify them, their friends or their location.

7.0 Managing Video Conferencing and Webcam use

- When available, video conferencing and webcam use will be appropriately supervised for the pupils' age.

8.0 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others may have internet access which may not include filtering. These may not be used in school. (See Section 12, should such devices be brought to school inadvertently.)

9.0 Protecting Personal Data

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

10.0 Procedures

- The school IT system's security will be reviewed regularly by the E-Safety Lead.
- Virus protection will be updated regularly.
- Acceptable use posters will be displayed in rooms where internet access is available.
- The school will work in partnership with parents, the LA, DfE, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT subject leader and the school Network Manager and the E-Safety Lead informed. These staff must consider whether to report the event to the Local Authority and/or the child protection organisations listed in Section 12.
- Any concerns about the suitability of sites will be reported to SWGfL by the E-Safety Lead or senior management team.
- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access.
- The school should audit IT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.
- E-Safety training will be embedded within the IT scheme of work or the Personal Social and Health Education (PSHE) curriculum.
- Staff will always use a suitable and safe search engine when accessing the web with pupils.

- Staff will be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone.
- Should special circumstances arise where such communication is felt to be necessary, the agreement of the Head Teacher should be sought first and appropriate professional language should always be used.
- Staff must not generally use mobile phones during teaching time whilst at the school or during off-site visits or activities but we recognise that this may occasionally be necessary.

11.0 Handling E-safety Complaints

- Complaints of internet misuse will be dealt with by the Head Teacher or senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see the school's Complaints Procedure).
- Pupils and parents will be informed of consequences for pupils misusing the internet.

12.0 Enlisting Parents' and Carers' Support

- Parents and carers attention will be drawn to the school E-Safety Policy.
- E-Safety information for parents is available from a number of sources, such as: Childnet (www.childnet.com), Think u Know (www.thinkuknow.co.uk), the South West Grid for learning (www.swgfl.org.uk), the UK Safer Internet Centre (UKSIC) (www.saferinternet.org.uk), the Child Exploitation and online Protection Centre (CEOP) (www.ceop.police.uk), the UK Council for Child Internet Safety (UKCCIS) (www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis), the Gloucestershire Safeguarding Children Board (www.gscb.org.uk) and the Internet Watch Foundation (www.IWF.org.uk).
- The school will ask all parents and pupils to sign the parent/pupil agreement at the start of each school year or when children are admitted in the case of in-year admissions.
- The present E-Safety Policy is limited to usage of the school's computing and communications equipment. The school would prefer parents and carers not to allow pupils to bring into school: mobile 'phones, electronic games consoles or any other device capable of internet connection. Should this occur, then the school takes no responsibility for the communications or material received or sent out, or for any financial or legal charges arising from the use of such non-school devices. However, the school does understand that there may be times when parents or carers might have a reasonable need to communicate directly with a pupil in school. Parents and carers are responsible for the parental controls settings of any communications devices that pupils bring into school. Devices should not be active during school time. The school takes no

responsibility for the loss of, or damage to, any such device brought to school by a pupil, parent or carer.

13.0 Rules for Acceptable Internet Use

- The school has installed computers and internet access to enhance learning.
- The rules for school computer and internet use and pupil/parent/carer agreement forms are provided in the CHS Policy: Acceptable use of IT policies. These also provide a form for reporting any unsuitable material encountered.
- Rules for adults are given in the CHS Code of Conduct for I.T. for all adults working with children.

14.0 Related Policies

The present policy is related to other Cam Hopton Church of England Primary School policies, as listed below:-

- Behaviour.
- Anti-Bullying
- CPSHE
- Acceptable use of ICT
- Code of Conduct for all adults working with children.
- Complaints Procedure.
- Safeguarding and Child Protection.

Cam Hopton CE Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

This school aims to serve the community by providing high quality education and promoting Christian Values.