

Holy Trinity C. E. (Aided) Primary School

Social Media and e-Safety Policy

Statement of definition

E-Safety is a child protection issue not an ICT issue and this policy should be considered in partnership with the school's safeguarding policies. All people working in school, whether adult or child have a duty to be aware of e-safety at all times and to know the required procedures in this policy and to act on them.

E-safety is not limited to school premises, school equipment or the school day. Neither is it limited to equipment owned by the school. E-safety is a partnership concern between the school, pupils, parents and carers, network providers and other local agencies.

Statement of duty of care

The *Headteacher* in conjunction with the *Leadership Team* will have responsibility for all e-safety matters.

All staff are responsible for supporting e-safe practices in schools.

Pupils at all levels need to understand their responsibilities and liabilities in the event of deliberate attempts to breach e-safety protocols.

Scope of policy

E-safety concerns the day to day running of the physical network and information passing through it whether connected via the internet, virtual private networks, intranets or local area networks. E-Safety also covers technology and networks not owned by the school.

Pupils will be taught safe practices and the e-safety policy will be monitored and enforced.

This e-Safety policy contains the school's Acceptable Use policy.

All instances of e-safety, whether by direct observation or disclosure will be taken seriously.

The process to be followed in the event of a breach of e-safety is detailed in Appendix 1.

If parents, carers, governors or other adults require further support with understanding e-safety issues in school, please visit our school website:

<http://holy-trinity-cuckfield.eschools.co.uk/website>, or if you wish to discuss anything in person please contact the Headteacher through the school office.

Managing Internet Access

Information system security

- Servers are located securely and physical access to the server room is restricted.
- The server operating system is secured and kept up to date by the ICT technician.
- Personal data sent over the Internet will be encrypted or otherwise secured. e.g. AVCO

School ICT systems security will be reviewed regularly.

Virus protection is updated each time a machine logs on to the server.

Security strategies will be discussed with the Local Authority.

Holy Trinity CE(A) School uses

- Microsoft 365 Outlook email system

Part 1 - Teaching and Learning

The Internet and related technology has become a rich and vital part of education, work and home life. This powerful technology is always developing, changing and growing and whilst this is exciting it also presents challenges and dangers we must address.

At Holy Trinity CE(A) School, we believe that the benefits to pupils from access to the resources available via 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.

Using the Internet for Education

Internet use will enhance learning

- 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 how to report unpleasant Internet content

The benefits include:

- access to a wide variety of educational resources including libraries, art galleries and museums
- rapid and cost effective world-wide communication
- gaining an understanding of people and cultures around the globe
- staff professional development through access to new curriculum materials, experts' knowledge and practice
- exchange of curriculum and administration data with LA/DFE
- social and leisure use

- greatly increased skills in Literacy, particularly in being able to read and appraise critically and then communicate what is important to others

All staff will review and evaluate resources available on web sites to ensure these are appropriate to the age range and ability of the pupils being taught. The ICT Subject Leader will assist in the dissemination of this information.

Pupils' Access to the Internet

We will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff are aware of the potential for misuse, and will be responsible for explaining our expectations to pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- 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, retrieval and evaluation.

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible we provide pupils with suggestions for suitable sites across the curriculum. Staff will always check the suitability of websites before suggesting them to children or using them in teaching.

Unsuitable material

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 a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

Despite the best efforts of the school occasionally pupils may come across something on the Internet they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur so action can be taken.

Such action will include:

- Making a note of the website and any other websites linked to it.
- Informing the ICT Subject Leader and Deputy Headteacher
- Logging the incident (see appendices)
- Informing the LA/ISP so the website can be added to the content filter if appropriate (*contact the ICT helpdesk*)
- Discussion with the pupil about the incident and how they might avoid similar experiences in the future.

Teaching safe use of the Internet

We think it is crucial to teach pupils how to use the Internet safely both at school and at home. We use the Kidsmart safety code to support our teaching in this area:



We will have e-safety theme weeks in addition to using the LA, Kidsmart, ThinkuKnow and CEOP materials as part of planned teaching and assemblies to all year groups.

Online bullying and harassment

Online bullying and harassment via mobile phones, instant messaging, social networking sites, e-mail and chat rooms are unacceptable and can have a serious effect on pupils and staff. We use a variety of strategies to help prevent online bullying including:

- Specific teaching about Cyberbullying;
- No access to public chat rooms, instant messaging services and bulletin boards;
- Teaching pupils how to use the Internet safely and responsibly;
- Encouraging pupils to discuss any concerns they have about online bullying with staff.
- Posts on the school website should be approved by teachers before being published.

Internet-enabled mobile phones and handheld devices

More and more young people have access to internet enabled devices such as WAP phones, camera phones and PDAs. Whilst we recognise the potential advantages these devices offer we do not believe the use of such devices in school is appropriate especially given they can potentially allow information and pictures to be posted remotely to a web site.

- Pupils are not allowed to carry or use mobile phones on school premises for any purpose unless supervised by a member of staff.
- Pupils must under no circumstances upload pictures taken at school to a public website.

Expectations of Pupils using the Internet

- All pupils are expected to read and agree the school's Acceptable Use Agreement.
- At Holy Trinity CE(A) School, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. They have been taught the rules of etiquette in e-mail and are expected to follow them.
- Pupils must ask permission before accessing the Internet
- Pupils must not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No personal information such as phone numbers and addresses should be given out and no arrangements made to meet someone.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

Downloading files and applications

The Internet is a rich source of free files, applications and other materials that can be downloaded and installed on a computer. Whilst some of the material may be useful, much is inappropriate and may adversely affect the performance and reliability of school equipment.

- Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.
- With the exception of sites providing copyright free teaching resources, staff are not allowed to download files from the Internet without permission from the ICT Technician.

Portable media

Pupils are encouraged to carry out tasks at home and bring them in to share with the class. Portable media such as CDs and Memory Sticks are a common way of transferring viruses between computers. Our virus protection software will scan such media and warn of any viruses. Such media should only be introduced to machines that have been recently updated with the latest virus protection.

Photographs

Whilst in school children will have access to technology that allows them to take video and photographic images. Children must use these responsibly and only takes images of other children for use in school work appropriately and with other children's consent. Children should be made aware that they are responsible for the use of this technology.

E-mail

E-mail is a valuable method of communication which plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail and how to use it appropriately and effectively.

Pupils are taught that e-mail messages sent using a school account will represent the school as well as the pupil and that they should act respectfully and appropriately at all times. Pupils are told that e-mail may be monitored for safety reasons although privacy will be respected as far as possible.

Pupils are not allowed to access personal e-mail using school internet facilities due to the quantity of unsolicited e-mail, unsuitable content and virus threats associated with commercial e-mail accounts.

Website

A web site can celebrate good work, promote the school, publish resources for projects and homework, and link to other good sites of interest.

- Children's pictures will only be used with permission but will never include their name.
- Home information and e-mail identities will not be included only the point of contact to the school i.e. phone number, school address and office e-mail address.
- Group photos will not list names
- Work displayed will be of the highest quality and reflect the status of the school.

As part of the ICT and wider curriculum pupils may be involved in evaluating and designing web pages and web related resources.

Any work that is published on a public website and attributed to members of the school community will reflect our school and therefore will be checked carefully for mistakes, inaccuracies and inappropriate content.

Where pupils' websites are published on the wider internet as part of a project any identifying information will be removed and images restricted.

Social networking and personal publishing (see Social Media Policy)

The school will control access to social networking sites, and consider how to educate pupils and their parents in their safe use, but ultimately outside of school it is parental responsibility to check their own children's use of these sites.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Pupils will be advised to use nicknames and avatars when using social networking sites.

Pupils will be reminded about the legal age for using social network and media and why these limits have been put in place.

Children will be advised that anything they (or anyone else) publish on the internet or via social media is then in the public domain and can remain in use even once they have removed it.

Internet Use Agreements

All pupils and their parents / guardians and staff are asked to read and sign an agreement covering the expectations when using the Internet in school. Copies of the agreements are available from the school.

How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia.

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

Virtual classrooms and virtual communities widen the geographical boundaries of learning. New approaches such as parent access to assessment scores are being investigated.

Holy Trinity CE(A) School Primary School aims to keep up to date with new technologies, including those relating to mobile phones and hand-held devices, and be ready to develop appropriate strategies.

Part 2 – Policy for staff use

This section of the policy refers specifically to staff/ adult use of ICT at Holy Trinity CE(A) School Primary School. Statements in this section are *in addition* to Part 1.

Staff use of the Internet

At Holy Trinity CE(A) School Primary School, we understand that the Internet is a valuable resource for staff. It provides a wealth of resources, teaching materials and information that teachers can use to enhance the curriculum. It allows staff to share resources with other schools and to engage in debate and discussion on educational topics.

It also provides an efficient way to access information from the LA and government agencies that will help staff keep abreast of national and local developments.

We are committed to encouraging and supporting staff to make the best use of the Internet and all the opportunities it offers to enhance teaching and support learning.

To enable staff to make full use of these important resources the internet is available to all staff for professional use. All staff using the school's internet facilities will be asked to sign the acceptable use agreement.

There are serious implications for staff who deliberately misuse the Internet which could result in disciplinary action.

Professional Use

Staff must model good Internet use where pupils are present as part of our ongoing commitment to encouraging safe and appropriate use.

When pupils are present in a classroom, staff may only access the Internet for professional purposes.

Internet use in class should be directly related to the class learning objectives.

Staff should ensure that they represent the school in a professional and appropriate way when sending e-mail, contributing to online discussion or posting to public websites.

School Laptops

Teachers who take laptops home to work should be aware that these are open to attack unless virus definitions are updated regularly. Spyware can transmit data from the laptop back to unknown sources.

- Staff taking school equipment home must ensure that it is not used by non-school staff. Use of school property by non-school personnel breaches the acceptable use policy and may give rise to unacceptable material being stored in the device.
- All staff using school laptops at home for periods of longer than one week must bring them into school and connect to the domain in order for the virus definition files to be updated.

The user must ensure that all wireless networks to which this equipment is to be connected must be securely encrypted. (WEP 64 bit as a minimum, with WPA being preferred).

Portable media

Portable media such as CD-ROMS and personal hard drive devices are a common way of introducing a virus or other undesirable agent into a school computer system. Staff should be mindful of this when transferring data from one machine to another.

The virus protections software is designed to scan CDs and other portable devices. If a warning is given do not continue and inform the ICT technician immediately.

Memory sticks are a valuable to transport data to and from the school premises. Any data containing children's names or sensitive school material must be password protected or on a secure memory stick. (teaching staff have been provided with secure memory sticks for this purpose)

Internet-enabled mobile phones, handheld devices and cameras

More and more people have access to internet enabled devices such as WAP phones, camera phones and PDAs. Whilst we recognise the potential advantages these devices offer we do not believe the use of such devices in school is appropriate especially given they can potentially allow information and pictures to be posted remotely to a web site.

- Staff are not allowed to carry or use mobile phones, personal cameras or other handheld devices on school premises for any purpose where children are present.
- Staff must under no circumstances upload pictures taken at school to a public website.

E-mail

E-mail is a useful and efficient professional communication tool and we encourage staff to use it where appropriate for communicating with colleagues, organisations, companies and other groups. To facilitate this staff members are given a school e-mail address which can be used for professional purposes.

Staff are reminded that using this e-mail address means they are representing the school and all communications must reflect this. They should only use this account for school related communications.

Outside of contractual working time, staff may access private e-mail accounts for personal use but must not download any attachments, pictures or other material onto school computers. The forwarding of e-mail chain letters and similar is forbidden.

Online discussion groups

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin boards to share good practice and disseminate information.

The use of such online forums relating to continuous professional development is encouraged although staff are reminded that they are representing the school and appropriate professional standards should be maintained at all times.

The school Internet facilities may not be used for personal access to public discussion groups, chat rooms or instant messaging.

Social networking and personal publishing

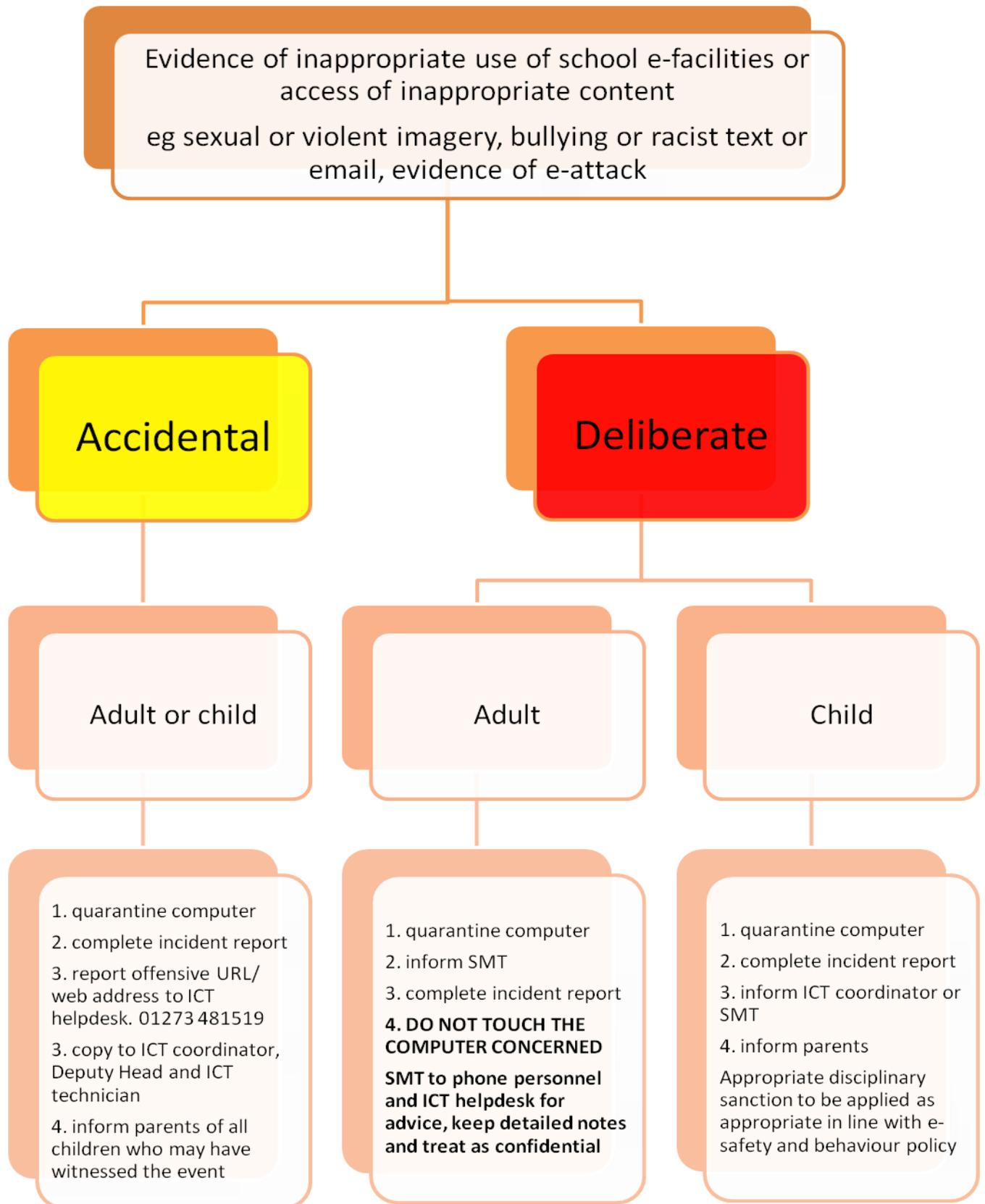
Staff are advised that the use of social network spaces brings a range of dangers both to the individual and the reputation of the school. Clear boundaries between professional and personal life on sites such as Facebook are expected to be maintained.

Staff are advised never to give out personal details of any kind which may identify them or their home. Staff are expected to avoid referring directly to the school.

On the school network, staff may not use social networking sites for personal use.

Reviewed by Staffing, Curriculum & Spirituality Committee Nov 2014; May 2017

Appendix 1



Appendix 2

Date of incident	
------------------	--

Name of member of staff discovering the incident				
Names of adults/ children involved				
Nature of incident	Access to inappropriate material	Cyberbullying	Grooming	Other inappropriate use
Details				
The event occurred...	...during a lesson	...in unsupervised time	...outside of teaching hours	...offsite
Location				
Does the event warrant police involvement? YES if...	...grooming.			
	...deliberately accessing/ uploading violent or pornographic images			
	... inappropriate sharing of images of children or their personal details			
	... other illegal activity			

Informed...	✓ & date/ time
Parents	
SMT	
ICT coordinator	
ICT Technician	

Action taken	date/ time/ name of contact
ICT helpdesk informed/ website blocked	
Advice sought from Personnel Contact	
Police contacted	
Disciplinary sanction applied	

Notes