Church Aston Infant School

E-Safety Policy
(Including Acceptable Use Policy for Pupils and Acceptable Use Policy for Staff)

March 2018

Telford & Wrekin
COUNCIL

Contents

Date Document Created	Date approved by Governing Body	Date of next Policy Review
May 2016	23 May 2016	March 2017
Reviewed: March 2017	21 March 2017	March 2018
Reviewed: March 2018	28 March 2018	March 2019

This E-Safety Policy relates to other Church Aston Infant School policies including:

- Computing Policy
- Anti-bullying Policy
- Behaviour and Discipline Policy
- Data Protection Policy
- Safeguarding and Child Protection Policy
- Telford and Wrekin Email and Internet Usage Policy
- West Mercia Consortium Raising Awareness in the Safe Use of ICT Systems at Home and in the Workplace
- School Security Policy
- Home School Agreement
- Photograph and video permission forms

This policy builds on the CEOP, Think U Know programme, NSPCC materials and Keeping Children Safe Online (KCSO). A survey by Ofcom, UK Children's media literacy 2009 interim report found that 66% of 5-7 year olds use the internet at home - with at least 30% using it for games. Additionally, over 85% have access to games consoles that may have online 'gaming' or 'chat' facility when linked to the Internet.

See Appendix A for an explanation of the safety risks involved with online technologies.

Teaching and Learning:

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience.

Internet use is part of the statutory curriculum and necessary tool for staff and pupils.

The school Internet access is designed expressly for pupil use and includes filtering of content. E-safety will be promoted and developed through assemblies, computing lessons, PSHE and circle times. Consideration and respect is given to the pupils' age, ability and developmental stage.

Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to report unpleasant Internet content. They will be shown how some people can pretend to be someone else and use social media to commit crime, bully and abuse others.

Managing Internet Access:

School ICT Systems and Usage

School ICT systems security will be monitored and reviewed regularly. Virus protection is updated and monitored regularly by Telford and Wrekin Local Authority. All use of school computer systems is in accordance with the Telford and Wrekin Email and Internet Usage Policy.

Email

Pupils may only use approved email accounts on the school system and email usage should be supervised and monitored by a member of staff.

Pupils must immediately tell a teacher if they receive any offensive email. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

Incoming emails should be treated as suspicious and attachments not opened unless the author is known.

Published Content and the School Website

The contact details on the website should be the school's address, email and telephone number. Staff or pupils' personal information will not be published.

The Headteacher, will take editorial responsibility and ensure that content is accurate and appropriate.

Photographs that include pupils will be selected carefully, ensuring that parents' wishes about their publication are adhered to.

Pupil's full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained for all pupils allowing the school to take photographs for education purposes and celebration on the school's website.

Parents are made aware that pupils' work may be published on the website.

Social Networking and Personal Publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use. Newsgroups and forums will be blocked unless a specific use is approved.

Pupils will be strongly and frequently reminded never to give out personal details of any kind that may identify them, their friends or their location. Pupils and parents will be advised through meetings, parent's evenings and newsletters that the use of social network spaces outside school is inappropriate and may bring a range of dangers for primary aged children.

Managing Filtering

The school will work with the Local Authority and Internet service provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the Headteacher immediately. Regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.

Mobile phones must be stored securely out of the classroom and are not allowed to be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protection Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Church Aston Infant School is registered with the Information Commissioner's Office.

Communication of the Policy:

Pupils and the e-Safety Policy

E-safety rules and Acceptable Use Policy for Pupils will be discussed with the pupils throughout the computing curriculum in the Digital Literacy strand. Pupils will be informed that network and Internet use can be and will be monitored regularly.

Staff and the e-Safety Policy

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. They will be asked to sign the Staff Acceptable Use Policy at the start of the academic year and before being allowed to use any school PCs, laptops, iPads or tablets.

Enlisting Parents Support

Parent's attention will be drawn to the school e-safety guidance in newsletters and the school prospectus.

Policy Decisions:

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 may leave or pupils' access be withdrawn.

Assessing Risks

The school will take all reasonable precautions to ensure that users access only appropriate materials. Due to the scale and linked nature of the Internet content, it is not possible to guarantee that unsuitable material will never appear on a piece of equipment linked to the school network. The school cannot accept liability for the materials accessed, or any consequences of Internet access.

Responding to a Report of Abuse

It is important to acknowledge that discussion about e-safety may raise issues for children about their own or others abusive experiences and this may be related to sexual abuse and/or internet related crime. If a pupil reports abuse or a concern then this should be dealt with following the Safeguarding and Child Protection procedures with a Concern Form being completed with accurate factual notes and this being forwarded to a Designated Safeguarding Lead immediately.

Handling e-Safety Complaints

The Headteacher will deal with complaints of Internet misuse. Any complaints of staff misuse must be reported immediately. Complaints of child protection nature must be dealt with in accordance with the Safeguarding and Child Protection Policy.

Pupils and parents will be informed of the complaints procedure and will be informed of the consequences for pupils misusing the Internet.

If necessary discussions will be held with West Midlands Police Youth Crime Reduction Officer for advice, guidance or to establish procedures for handling potentially illegal issues.

Acceptable Use Policy for Pupils

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people who I know in real life
- tell an adult if anything makes me feel scared or uncomfortable
- make sure all messages I send are polite
- show an adult if I get a nasty message
- not reply to nasty messages or anything that makes me feel uncomfortable
- talk to my teacher before using anything on the Internet
- not tell people about myself online, my name, anything about my home, family or pets.
- not load photographs of myself onto the computer
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

Acceptable Use Policy for Staff

I agree that I will:

- use personal data securely
- implement the school's policy on the use of technology and digital literacy
- educate pupils in the effective use of the internet
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified
- set strong passwords
- report unsuitable content or activities to the Headteacher

I agree that I will not:

- visit Internet sites, make, post, download, upload or pass material, remarks, proposals or comments that contain or relate to:
  - pornography (including child abuse images)
  - promote discrimination of any kind
  - promote racial or religious hatred
  - promote illegal acts
- breach any Local Authority / School policies
- do anything that exposes children to danger
- forward chain letters
- breach copyright law

I accept that my use of the school and Local Authority ICT facilities may be monitored.

Signed: …….. Date: ……

APPENDIX A

Explanation of the safety risks involved with online technologies
(Think U Know and CEOP)

What is Sexual Grooming?

Often, adults who want to engage children, or talk to them for sexual gratification will seek out young people who desire friendship. They will often use a number of grooming techniques including building trust with the child through lying, creating different personas and then attempting to engage the child in more intimate forms of communication including compromising a child with the use of images and webcams. Child sex abusers will often use blackmail and guilt as methods of securing a meeting with the child.

What is Cyberbullying?

Cyberbullying is the use of e-mail, instant messaging, chat rooms, mobiles, or other forms of information technology to deliberately harass, threaten, or intimidate someone. Cyberbullying is often done by children, who have increasing access to these technologies; though may not understand the impact such actions can have on others because they can't see them. However, it is by no means confined to children. The problem is compounded by the fact that a bully can hide behind an electronic veil, disguising his or her true identity. This makes it difficult to trace the source, and encourages bullies to behave more aggressively than they might face-to-face. Cyberbullying can include such acts as making threats, sending provocative insults or racial, homophobic or ethnic slurs.

Below are a range of communication mechanisms and an explanation of the risks they can pose to young people:

Social Networking

Social Networking websites utilise applications that help connect friends using a number of tools like blogs, profiles, internal email systems and photos. Well known sites include Bebo, Myspace, Facebook, and these have become an influential part of contemporary culture.

Although chatting online can be great fun, young people can sometimes find themselves in situations where they can feel out of their depth. Risks can arise when young people give out their personal details to strangers. The online world can often seem very different to the real world for young people, and they can be tempted to say and do things that they wouldn't dream of if they met someone face-to-face. This can include giving out personal information such as mobile numbers and pictures of themselves. Paedophiles are very clever at piecing together small bits information to track children down in the real world.

If they are talking to another child there is a risk that they will misuse this information - for example, by texting abusive messages to the child, or by posting their image on a website; but there is obviously a greater risk if the person that they are chatting to is an adult.

Chat rooms and Instant Messaging (IM)

A chat room is an online forum where people can communicate by broadcasting text-based messages in people on the same forum in real time. Sometimes these venues are moderated either by limiting who is allowed to speak (not common), by enabling users to report inappropriate posts to the

website's facilitator or by having moderation volunteers patrol the venue watching for disruptive or otherwise undesirable behaviour.

Instant messaging (IM) is a form of real-time text-based communication conveyed over a network, such as the Internet, between two or more people on a user's contact list. Examples include Windows Live Messenger, Jabber, ICQ and AIM. IM technologies often include additional features that make them even more popular such as having the ability to talk directly for free; to share files; or to view the other party through a webcam.

Young people will often 'swap friends' through Instant Messaging (IM), and therefore can be chatting to strangers who they feel they trust because a friend of a friend knows them. IM is a very intimate form of communication - more so than a chat room with many participants, and therefore child abusers will often use this as a means to extract personal information from a young person.

Mobile

Apart from young people spending all their time chatting to their friends, there are some risks in their use of mobile technology. A large proportion of new mobile phones have web access, and more recently - mobile TV has been launched. This means that young people can access content from the Internet and TV wherever they are, and without parental or teacher supervision. With the advent of picture and video messaging - young people need to be increasingly careful about the images they share. It is very easy for inappropriate images to be shared around a number of phones, changed and even put online, where it is impossible to get back. This is particularly worrying, if images are used in child abuse sites. Young people also need to be aware that they put themselves at risk of mobile bullying, or inappropriate intimate contact if they give out their mobile number to people they don't fully trust.

Gaming

Gaming sites can be fantastic fun for young people, however as with any online technology - there are risks.

5-7 year olds regularly look at such sites as:

Cbeebies site: http://www.bbc.co.uk/cbeebies/games/
Disney's Club Penguin: http://www.clubpenguin.com
Miniclip: www.miniclip.com/

The three main risks are:

Addiction

Online gaming can occasionally be addictive for young people. They can become so involved in the gaming communities (where you play against other users rather than the computer) that they lose touch with their offline friends, in favour of spending time with online users playing games. Young people often spend hours every night playing games, especially when their parents have gone to bed. For this reason, CEOP recommends that the computer is kept in a family room.

Abuse
Some young people who use online games can be abusive to other gamers. This can range from saying nasty things if there is a chat facility within the gaming site, to always winning and not sharing cheats

or knowledge on how to progress to the next level. Young people should be encouraged that when they play online games, they treat others how they would like to be treated.

Risky Behaviour

There are some young people who engage in risky behaviour to obtain cheats or knowledge to progress within a game. Adults with a sexual interest in children will encourage them to engage in inappropriate behaviour for rewards including sexual acts via webcam or sex chat. Young people need to understand that their online behaviour has offline consequences and that if someone engages them in a sexual manner online that they should inform a trusted adult immediately.