Holy Trinity CE Primary School

Online safety Policy

September 2016

Writing and reviewing the online safety policy

The Online safety Policy relates to other policies including those for Computing, bullying and for Safeguarding.

The school's named Online safety Coordinator is: Mrs. Hannah Martin

Our Online safety Policy has been written by the school, building on advice received and government guidance. It works in conjunction with the school devised acceptable use policy. It has been agreed by senior management and approved by governors.

The Online safety Policy was revised by Judith Driver and Hannah Martin

Created: September 2016
The next review date is: September 2017

The school will monitor and enforce the policy through: e.g.

- Teacher planning
- Policy Central – monitoring of network activity for laptops and desktops (mobile technology not covered)
- Log of any incidents (Judith Driver monitors this)
- E safety team at Walsall Education
- Technical Staff to ensure all security software, including virus software and settings are kept up to date (Symantec N Point – updates regularly)

Every member of the school community has a duty of care to e- safety as part of safeguarding. This policy deals with incidents associated with the use of technology that affects our school community.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online safety responsibilities. Incidents that occur outside of school are covered by parent's duty of care.

Monitoring Software

Policy Central is used across the network in order to

- Monitor inappropriate use of language
- Monitor internet usage Inc. words associated with the prevent agenda
- Enforce the agreement of the Acceptable Use Policy

Online Safety in the curriculum

A programme of training in online safety will be taught to children across the school from Nursery to Year 6, half termly. Online safety training will be included within the Personal Social and Health Education (PSHE) curriculum and children will be reminded at the beginning of any session using ICT.

Early Years Foundation Stage and Key Stage 1

At this level, use of the Internet will either be quite heavily supervised or based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Lower Key Stage 2

Children will now be given more opportunities to develop their digital literacy skills (e.g. sending polite and friendly messages online to other children, the need to create strong passwords etc). They will be shown how to develop a responsible attitude towards searching the World Wide Web and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Upper Key Stage 2

Children will now be encouraged to become more independent, agreeing to the acceptable use policy first, before searching for information on the World Wide Web using a child friendly search engine, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies. They will be encouraged to use technology safely and made aware of reporting anything suspicious to an adult.

Parents and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Primary will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website / pupil records
- Their children's personal devices in the school (where this is allowed)

Where an incident occurs within school the child's parents will be given appropriate advice for the use of technology at home.

Visitors to school

Whilst the nature of a visitor's Internet use will clearly vary depending upon the purpose of their visit, it is still important to explain the school's expectations and rules regarding safe and appropriate Internet use to them. These differ slightly to those given to pupils to acknowledge the different situations in which visitors will likely be using the Internet:

- I will respect the facilities on offer by using them safely and appropriately.
- I will not use the Internet for: personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect myself and others.
- I will not download/install program files to prevent data from being corrupted and to minimise the risk of viruses.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details for websites with others.
- I will not carry out personal or unnecessary printing when using the Internet due to the high cost of ink.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

These will be on a paper copy and signed by the visitor

E-communication within school

Staff should use a school email communication for anything work related and no other email address. The forwarding of chain communications is not permitted.

Mobile phones

The use of mobile phones should not be in the classrooms especially during the school day (8.50 - 3.15) excluding lunchtimes in the staff room or office, and only used on school trips away from children, in an emergency.

Digital images in the school community

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupil's instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images. Parents will be reminded of this at the beginning of any events where they are able to take images/videos.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the school policy concerning the sharing, distribution and publication of those images which prohibits such activity. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed (e.g. school uniform or PE kit) and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission. For example, a child must ask another before taking their photo.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names (First names and last initial only) will not be used anywhere on a website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

- Pupil's work can only be published with the permission of the pupil and parents or carers.

Social networking and personal publishing

The school will control access to social networking sites, they will be restricted as appropriate. Pupils will be educated in the safe use of such sites alongside the use of relevant child friendly websites.

Pupils, staff 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. Staff must not make 'friends' or communicate with current pupils or pupils that have left on any social network site, i.e. Facebook. Staff should check that their privacy setting is set to 'Friends only' and consider changing their profile name. Staff who choose to use 'Facebook' and other network sites do so at their own risk and should be aware of the School's Code of Conduct.

Pupils will be taught when 'gaming' i.e. on Nintendo Wii, they should only communicate with people they know rather than unknown gamers.

Managing filtering

The LA ICT and policy central will work with to ensure systems to protect pupils are reviewed. If staff come across unsuitable on-line materials, the site must be reported to the online safety Coordinator. If pupils come across unsuitable on-line materials, the site must be reported to their teacher who will inform the online safety Coordinator. Staff **are** now able to access sites such as 'You Tube' and others on request but staff need to be aware that these sites do contain inappropriate materials and therefore children are not allowed to use these sites. **Links and content should be checked in school just prior to use in the classroom due to daily rotation of advertising content.**

Managing 21st century technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. **School staff should be aware that mobile technologies with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.**

Mobile technology will be assigned to a child at the beginning of the school year and they must use the same equipment every lesson they log in. In exceptional circumstances where this is not possible a log sheet should be completed for the session and placed in the 'Ipad log folder' located in the staff room.

Personal devices, including mobile phones, will not be used during lessons or formal school time unless express permission is given by the head or SMT. Personal devices must not be accessed (e.g. in another room or locked away) when children are present. The sending of abusive or inappropriate messages or files by Bluetooth or any other means is forbidden. Staff will be issued with a school phone where contact with pupils is required. **Staff will not use personal devices to capture images/videos of pupils.**

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Refer to the School's data protection policy. Staff will be given access to a remote system to access data. This should be the only form of data storage that staff use. **Staff should ensure that the device is not left unattended whilst logged in. Staff should not walk away from any device without first locking it.**

Authorising Internet access
Parents will be asked to sign and return a consent form, then kept on file.

Handling Online safety complaints
Complaints of internet misuse will be dealt with by an e safety coordinator or a senior member of staff. Any complaint about staff misuse must be referred to the LADO.
Complaints of a safeguarding nature must be dealt with in accordance with school's safeguarding procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet.

Staff and the online safety policy
All staff will receive in house online safety update training on an annual basis. Staff are informed that network and internet traffic will be monitored and can be traced to the individual user. Staff will always use a child friendly safe search engine when accessing the web with pupils, for example http://www.awesomelibrary.org/

Staff that manage filtering systems or monitor ICT use will be supervised by senior manager and work to clear procedures for reporting issues.