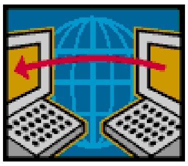
HOOLE CHURCH OF ENGLAND PRIMARY SCHOOL

E-Safety Policy

Policy Approved	**April 2019**
Review Date	**April 2020**
Responsible Staff	**R. Salisbury**
Governor	**J. Weaver**

E-Safety



E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile telephones, collaboration tools and personal publishing. It highlights the need to educate the pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy will operate in conjunction with other policies, for example Behaviour, Anti-Bullying, Teaching and Learning.

The school's e-safety Policy Guidance available on 360^{o} review tool forms the basis of this policy.

1.1 End to End E-Safety

E-Safety depends on effective practice at a number of levels:
Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

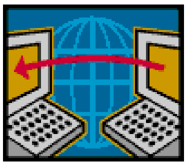
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Cheshire West and Chester Network including the effective management of filtering.
- National Education Network standards and specifications.

1.2 Further Information

Cheshire West area e-safety / Police Liaison Officer	amie.hough@cheshire.pnn.police.uk
E-safety materials and links	www.thinkuknow.co.uk/ www.ceop.police.uk www.net-aware.org.uk https://www.childnet.com/resources/kia/know-it-all-for-primary https://360safe.org.uk
Curriculum e-safety advice	https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/curriculum-planning
School ICT help	Dan Woolly dan@7elevensystems.co.uk
ICT filter	Securus

This e-safety policy is compliant with the 360^{o} e-safe approved guidance. Naturally, the policy must be translated into practice to protect pupils and educate them in responsible ICT use.

2.1 Writing and Reviewing the E-Safety Policy



The e-safety policy is part of the ICT Action Plan and relates to other policies including those for ICT, bullying and for child protection.

E-Safety Coordinator	Mrs Rebecca Salisbury	ICT Subject Leader
Designated Safeguarding Lead	Mrs Rosalind Flanders	Headteacher
Designated Safeguarding Lead	Miss Laura Sprowson	Inclusion Leader
Deputy Headteacher	Mrs Clare Watling	
Safeguarding Governor	Mr Andy Avery	
E-Safety Governor Lead	Reverend John Kirkland	School Governor

- Our e-Safety Policy has been written by the school, building on the E-safety 360° Review Tool approved e-safety policy guidance and government guidance. It has been agreed by senior management and approved by the school staff and governors.
- The e-Safety Policy and its implementation will be reviewed annually against e-safety measures through the online E-safety 360° self-review framework.

2.2 Teaching and Learning

The purpose of Internet use in school is to raise educational standards and to promote pupil achievements. The Internet helps to support the professional work of staff and enhance the school's management of information and business administration.

Internet services will be provided by Cheshire West and Chester Council.

2.2.1Why internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2.2How Internet use benefits education

- Access to world wide educational resources including museums and galleries.
- Access to experts in many fields for pupils and staff.
- Collaboration across support services and professional associations.
- Exchange of curriculum and administrative data with the Local Authority and DCSF.

2.2.3Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering managed by Cheshire West and Chester Council 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 and associated technologies so they understand the dangers and can make informed decisions both in and out of school.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Internet access will be planned to enrich and extend learning activities across the curriculum.

2.2.4 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 to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to search safely and effectively online using child-friendly search engines such ask www.safesearchkids.com or https://swiggle.org.uk As the children reach upper KS2, they will be taught of the potential dangers of using other search engines e.g. www.google.co.uk, how to ensure that they access suitable materials, and what to do if they find something inappropriate.
- Pupils will be taught the procedure of what to do if links to inappropriate web content occurs. Pupils should part-close the lid of their laptop then tell their teacher, who will record the URL address, time, date and content. This must be reported to the Local Authority school helpdesk via the Bursar and ICT Subject Leader.
- Pupils will be advised of the dangers of uploading material onto social networking sites. Pupils will be advised to be cautious of visiting sites recommended by friends if in doubt about the website's content.

2.3 Managing Internet Access

2.3.1 Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus Protection will be updated regularly.
- Security strategies will be discussed with Cheshire West and Chester Council.

2.3.2 E-Mail / Online messages

- Pupils may only use approved e-mail accounts set up by their class teacher as part of their learning and will only contact users stated by their teacher.
- Pupils must immediately tell a teacher if they receive offensive e-mail / message / comment when they have logged into their area of the school website. They can do this by clicking the red 'Report something to a teacher' button, which is located on their dashboard on the pupil area of the school website. This sends an alert to the website administrators who will alert the headteacher / ICT subject lead.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed notepaper. These emails should be sent via the teacher's email account.
- School email accounts should only be used for reasons related to school.
- The forwarding of chain letters is not permitted.

2.3.3 Published content and the school website

- The contact details on the school website should be the school address, e-mail and telephone number. Staff or pupils' personal information should not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The School Admin team are trained with which information can be published and which cannot.
- Children and staff should keep log-in details private.

2.3.4 Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs or videos of pupils are published on the school website. Staff need to ensure that they are aware of the photographing / recording permissions of the children in their class.
- Pupils' full names will not be used anywhere on the school website, particularly in associations with photographs.
- Photographs of the children can be uploaded onto the gallery area of the school website as it password protected and can only be accessed if the children / parents have a user account.
- Photographs and videos that include pupils will be selected carefully.

2.3.5 Social networking and personal publishing

- Cheshire West and Chester Council will block inappropriate social networking sites.
- Pupils will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils and parents will be advised of the dangers of social networking sites which children may access outside school.
- School staff must be aware that bullying can take place through social networking. Any instances of cyber-bullying will be dealt with as according to the school's anti-bullying policy.
- Children will be taught how to act responsibly and make informed decisions when accessing social networking sites.
- Staff should not become 'friends' with pupils on social networking sites or 'follow' pupils, for example on Instagram, Twitter, Facebook.
- As part of Safer Internet Day, children will have an assembly lead by Cheshire Police Schools Officer. This assembly covers general e-safety, but focuses on publishing personal data and social networking via online games. Parents will also be invited to a similar parent assembly.
- Staff should be aware that if they post on Twitter, their 'tweets' can be viewed by anybody, there are no security settings. This is similar on Instagram. The 'tweets' and posts should therefore not bring their professional role into disrepute.
- Staff should also be aware of implications and risks of using instant messaging services, such as Snapchat, and that they should make informed decisions when using the application.

2.3.6 Managing Filtering

- Filtering is coordinated through Cheshire West and Chester Council. Any inappropriate websites will be reported first to the Bursar, who will then contact Cheshire West and Chester Council through the help desk to be blocked.

2.3.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit before use in school is allowed.
- Mobile telephones will not be used during lessons or formal lesson time. The sending of abusive or inappropriate text messages is forbidden.
- Only Year 5/6 pupils will be allowed to bring a mobile phone to school. The children will be reminded that they should only bring a mobile phone to school if it is absolutely necessary e.g. they are walking home from school alone.
- If a pupil brings a mobile phone to school, it must be switched off the moment that they are on the school premises, and remain switched off during school hours until they are off the school premises.
- During morning registration, mobile phones will be placed into named envelopes and places in a basket which is then locked away in the Headteacher's office.
- Staff are not permitted to use their mobile phones in the presence of children. If they need to use their mobile phone during breaktimes, they must use it in the staffroom.
- Staff will be issued with a school phone for educational visits where contact with only the school, and other members of staff on the trip, during class visits is necessary.

2.3.8 Protecting personal data

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

2.4 Policy Decisions

2.4.1 Authorising Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resources and school laptops at home.
- All pupils must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resources.
- The school office 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 a pupil's access be withdrawn.
- Parents will be informed that pupils will be provided with Internet access via the Home School Agreement.

2.4.2 Assessing Risks

- Children will be supervised at all times when accessing the Internet and the school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Local Authority can accept liability for the material accessed, or any consequence of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

2.4.3 Handling e-safety complaints

- Complaints of any Internet misuse and/or cyber bullying will be logged on CPOMS and dealt with by a senior member of staff as laid out in the Anti-Bullying Policy.
- Any complaint about staff misuse must be referred to the Headteacher, in accordance with the Complaints Policy.

- 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.
    - Parents and children can report e-safety complaints by pressing the 'Report something to a teacher' button on the pupil dashboard when a pupil has logged into the school website, or by letting an adult in school know. These events will be recorded on CPOMs.
    - Complaints will be dealt with by the class teacher initially and then referred to the SLT and e-safety officer where appropriate.
    - If the child has breached the acceptable use agreement, they will have their user accounts for the school website deactivated for 2 weeks and parents will be informed.
- In the event of a reported e-safety risk the Headteacher, Safeguarding Leader and ICT Subject Leader will follow appropriate procedures as laid out in The Child Protection Policy.
- Children learn about cyber bullying and how to report it via PSHCE lessons, as part of their weekly computing sessions based on the Rising Stars Scheme of Work, workshops involving the Police Schools Officer and e-safety competitions organised by the Local Authority and School.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each sessions where the computers are to be used. Children will be able to give their views about staying safe online during these discussions.
- Instruction in being responsible and safe use for pupils will precede Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- E-safety will be progressively taught through curriculum delivery to raise awareness of safe Internet use as part of PSHE, Citizenship, ICT and the Heart Smart programmes respectively.
- Monitoring of e-safety practices and procedures will be through lesson observations and discussions with the children.

2.5.2 Staff and the e-safety policy

- All staff will sign an Acceptable Use Agreement
- All staff will be given the school e-safety policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Personal home Internet usage on school ICT equipment should be considered with caution. School ICT equipment will only be used at home for educational purposes e.g. planning and preparation.
- Staff development in safe and responsible Internet use and associated technologies and the school e-safety policy will be audited and provided as required.
- Staff and appropriate governors will attend annual workshops provided by the Police Liaison Officer to update their knowledge of e-safety.

2.5.3 Parents and the e-safety policy

- Parents' attention will be drawn to the school e-safety policy in newsletters, the school brochure and on the school website.
- Parents have access to the website and can view their children's work and actions.
- Opportunities will be provided for parents to learn about e-safety by the Police Liaison Officer during Safer Internet Day.

2.5.4 Governors

- Governors will be given a copy of the e-safety policy and its importance discussed.
- Governors will be asked to sign an Acceptable Use Policy.
- Governors will be kept informed of dangers and new and emerging technologies and encouraged to attend new and appropriate training.
- It is the governors' responsibility to monitor the e-safety policy and procedures used in schools.