Holbrook Primary School

E- Safety Policy

Holbrook Primary School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that E-Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones and wireless technology.

Electronic Communication includes:

- **Internet collaboration tools:** social networking sites and web-logs (blogs)
- **Internet research:** websites, search engines and web browsers
- **Mobile phones**
- **Internet communications:** e-mail and IM
- **Webcams and videoconferencing**
- **Wireless games consoles**

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

Holbrook primary School recognises and seeks to develop the skills that children need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

Risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

What are the risks?

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

The School's Safety Responsibilities

- Holbrook Primary School has a Designated Safeguarding Lead for all matters of child protection and safeguarding.
- The Subject Leader for Computing(SLC) has responsibility for the computing curriculum and this includes pupil education in e-safety. The SLC will also arrange for e-safety professionals to conduct training on an annual basis for pupils in Y5 and Y6, teachers, governors and parents.
- The SLC will ensure a leaflet of advice on ICT Safety is up to date and distributed to all parents.

- The SLC will ensure that e-safety posters are in place in all teaching areas and will hold colleagues to account where these posters are not in place.
- The governors will review this policy and the associated leaflet on a regular basis in line with the schedule of policy review. This policy may be reviewed as a matter of urgency in response to new information from government, the local authority or e-safety professionals.
- Advice to teachers and support staff will be given on a regular basis through safeguarding messages at meetings.
- Advances in technology may require new responses from the school. This policy will be reviewed to take into account any issues emerging from new technology.
- The School Business Manager and the SLC will review the filtering system with the provider to ensure it is fit for purpose.
- All incidents of possible misuse will be investigated.

Teaching and learning

Developing effective practice in Internet use for teaching and learning is essential. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning. 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.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. 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.

- 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.
- Teachers and support 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.

Evaluating Internet Content

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Local Area Network security

- Users must act reasonably
- Users must take responsibility for their network use. For all staff, flouting electronic use policy is regarded as a matter for dismissal
- Workstations should be secured against user mistakes and deliberate actions, e.g. deleting files and folders
- Servers will be located securely and physical access restricted
- The server operating system will be secured and kept up to date
- Virus protection for the whole network will be installed and kept up to date
- Access by wireless devices must be pro-actively managed

Wide Area Network (WAN) security

- All Internet connections must be arranged through the school's filtering system.

- Firewalls and switches are configured to prevent unauthorised access between schools.
- The security of the school information systems will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the LA when necessary
- Personal data sent over the Internet should be encrypted or otherwise secured
- Pupil names should not be included in emails between staff
- Portable media may not be used without specific permission followed by a virus check
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail
- Files held on the school's network will be regularly checked

Email

- Pupils do not have school email accounts
- If learning about emails in lessons, special accounts may be set up but these will be monitored by the teacher

School Website and Learning Platform

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Use of Images

Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless there is parental permission.
Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
Written permission from parents or carers will be obtained before images of pupils are electronically published.

Social Networking

The school will block/filter access to social networking sites such as Facebook. The school's Twitter account will be accessible in school.
Newsgroups will be blocked unless a specific use is approved.
Pupils will be taught about sources of support if they experience a problem online and will be taught key safety points:

- never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- not to place personal photos on any social network space
- consider how public the information is and consider using private areas
- background detail in a photograph which could identify the pupil or his/her location e.g. house number, street name or school

Teachers should not run social network spaces for pupil use on a personal basis.

Cyber-bullying

Holbrook Primary School will ensure cyber bullying incidents are recorded in the school anti- bullying log in line with the school's Anti- Bullying Policy.

Filtering

The school will work with the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to SLC.
The school's IT technician will ensure the filtering methods selected are appropriate, effective and reasonable.

Video Conferencing

Video conferencing will only take place under the supervision of a teacher or member of staff and will only take place on school premises. Unique log on and password details for video conferencing should only be issued to

members of staff and kept secure. Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Mobile Phones
Pupils must hand in to the school office any mobile phone they have brought to school. Phones can be collected at the end of the day. Members of staff do not have to hand in their mobile phones but these must not be used in classrooms or public areas.

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

Safety and Security of electronic equipment
All staff laptops are taken home in the evening, locked away or put away out of sight. All staff are aware these cannot be left in cars overnight.
All devices should be passworded.
Only passworded flash drives should be used for the storage of school data. These have been provided to all teachers.
Loss of equipment should be reported to the Head teacher immediately.
Staff should log off when the equipment is not in use.
At the end of the school day, class iPads are put away within the classroom or taken home by class teachers.
Class iPads are cleared of photos within 5 days of pictures taken to avoid losing any quantity of photos if the iPad was to be lost or stolen. This will allow EYFS staff time to upload images to Tapestry (our online EYFS pupil Learning Journals).

Internet Risks
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences resulting from Internet use.
The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
Methods to identify, assess and minimise risks will be reviewed regularly.

E Safety Complaints
Complaints of Internet misuse will be dealt with by a senior member of staff.
Any complaint about staff misuse must be referred to the Head Teacher, unless it is the Head Teacher where complaints will be sent to the Chair of Governors.
Pupils and parents will be informed of the complaints procedure.
Parents and pupils will need to work in partnership with staff to resolve issues.

Supporting Actions
- Safe internet use posters will be posted in all teaching areas of the school
- Families of Holbrook pupils will be provided with a leaflet of advice on ICT use
- E- Safety messages will be included in each newsletter and displayed on the playground screen
- E- safety content will form part of the computing curriculum
- An e-safety expert will talk to pupils in Y5 and Y6 on an annual basis
- There will be an annual meeting for staff, parents and governors on e- safety, led by an e-safety expert
- Cyber- bullying incidents will be recorded in the school's Anti- Bullying log in a separate section

This policy should be considered alongside other relevant policies, including Safeguarding Children Policy and Feeling Safe to Learn: An anti- bullying policy. It will be reviewed in line with the governing body's schedule of policy review.

Reviewed November 2017