Holly Grove Primary School Online Safety Policy

Online safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Holly Grove Primary School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger – knowingly or unknowingly – when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

"To ignore online safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving

children and young people vulnerable."

From: Safeguarding Children in a Digital World. BECTA 2006

Holly Grove Primary school acknowledges the assistance of Oakridge Primary School, Sheffield City Council and Kent County Council in providing content for this document.

1. Online safety Policy

Our online safety Policy has been written by the school, following government

guidance. It has been agreed by senior management and approved by governors.

- The online safety Policy and its implementation shall be reviewed annually.
- It has been approved by the Governors and will be reviewed in the annually as part of our safeguarding review

  Roles and Responsibilities Governors:

Governors are responsible for the approval of the online safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online

  safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety Co- ordinator.

- The Headteacher / Senior Leaders are responsible for ensuring that the online safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and Deputy Head should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

  The online safety co-ordinator:

- Takes day-to day-responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school ICT technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

2.Teaching and Learning

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

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, our digital footprint and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning

In line with the inclusion strategy published by Staffs County Council Education Service, Holly Grove Primary School provides equality for all its pupils. The school actively promotes a Dyslexia Friendly learning environment and is using teaching techniques suitable for all children to learn.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

Our SEN co-ordinator and individual teachers to ensure all children have equal access to succeeding in this subject.

3.Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to online safety and agree to its use:

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

4.World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an online safety Log, which will be stored in the Headteacher's office with other safeguarding materials.
- 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 are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

5.E-Mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of online safety:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

6.Social Networking

Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face- to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends and family over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

- Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.
- Staff will not be allowed to interact with pupils on social networking or media sites, unless it is in the context of teaching and learning.
- Staff will be encouraged not to interact with parents on social networking or media sites, unless it is in a professional context.

7.Mobile Phones/Devices/Smart Watches

Many new mobile phones/devices/smart watches have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.
- Pupils are not allowed to have smart watches in school unless permission gained from Headteacher regarding the reason for why the device is needed on site.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use school phone to contact parents.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom, whilst pupils are present.
- All staff, visitors and volunteers are to use the lockers in the office area to store mobile phones.
- Staff may use their mobile phones in the staffroom or school offices during the school day. After/before school staff can use mobile phones in their classrooms when there are no children on site. This is not permitted in the hall as Holly Berries After School Club use this space with children.
- Parents cannot use mobile phones on school trips to take pictures of the children.

9.Digital/Video Cameras

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff. • The Headteacher or nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

10. 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.

11. Published Content and the School Website/School Twitter Account

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Web site or Twitter account

- Parents may upload pictures of their own child only onto social networking sites. If the picture includes another child / children then it is their responsibility to gain permission from that child's parents.

- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

12. Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- Online safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

13. Protecting Personal Data

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

14. Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

15. Handling online 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 Headteacher
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

16. Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils are taught about the of the importance of being safe on social networking sites and being online generally through the different apps that are available as well as online gaming. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

• All staff will be given the School online 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.

Parents:

• Parents' attention will be drawn to the School online safety Policy in newsletters and on the school Website. They will receive updates on online safety through the school newsletter as well as an safety page on the school website with lots of user guides.

17. Further Resources

We have found these web sites useful for online safety advice and information.

http://www.hollygroveschool.co.uk/

http://www.staffsscb.org.uk/

http://www.thinkuknow.co.uk/
http://www.childnet-int.org/

DATE: Spring Term 2019

REVIEW DATE: Spring Term 2020