Hill View Primary School
The best in everyone™
Part of United Learning

ONLINE SAFETY POLICY

(previously E-Safety)

Reviewed December 2018

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. This policy details the procedures in place to support safe and responsible use of the internet by all members of the school community.

This policy has been developed, and will be monitored and reviewed, by the Safeguarding Committee of the Governing Body in consultation with parents, staff and pupils. The committee would like to acknowledge that SWGfL model policy was used during the development of this policy. Further information from SWGfL can be found here http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy

This Online Safety Policy works in conjunction with other policies, including those for ICT, child protection and safeguarding. The school's Online Safety is co-ordinated by the Designated Members of Staff for Safeguarding, with support from the Headteacher and ICT Leader.

This policy will be reviewed at least every two years but can be reviewed at any time in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents, governors and visitors) and for use both in and out of the school.

The Education and Inspections Act 2006 empowers the Headteacher to such an extent as is reasonable, to regulate the behaviour of pupils when they are on the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying (cyberbullying) or other online safety incidents covered by this policy, which may take place out of the school, but is linked to being a member of the school.

The school will deal with any incidents that fall under the remit of this, the anti-bullying and the safeguarding policies and will inform parents of incidents of inappropriate online behaviour that take place out of school.

Teaching staff:

- have an up-to-date awareness of online safety matters, know the current policy and follow good practice guidelines. They are kept up-to-date with information through staff INSET, guidance information and self-study.
- Abide by the Acceptable Use of ICT policy and the staff Code of Conduct
- Report any suspected misuse, by pupil or adult, to the Headteacher, School Business Manager or ICT lead as soon as possible
- ensure that any online communication with pupils or parents is professional
- ensure that online safety is planned for and embedded into their teaching
- monitor the use of digital technologies, mobile devices, cameras etc by pupils and adults and implement policies where applicable

All staff:

- will receive online safety training which is updated as new information or technologies arise. Training is refreshed each year as part of the annual safeguarding/health and safety/first aid review.
- when new, receive online safety information as part of their induction
- when new, receive the Acceptable Use of ICT and Online Safety policies as well as the Code of Conduct as part of their induction
- will be provided with advice, guidance or training as requested or as identified through performance management procedures.

Internet use by pupils is important:

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- All pupils read and must abide by the rules detailed in the school's "Pupil's online safety agreement" before using any school ICT resource. This will be relaunched in January 2019.
- 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.
- The purpose of the 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 information and business administration systems.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use by pupils will enhance learning:

- The school Internet access is planned expressly for pupils' use and includes filtering appropriate to the age of pupils.
- Pupils are 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.
- Staff guide pupils in on-line activities that supports the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content:

- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is part of every subject.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported, where appropriate, to the business manager or ICT leader, who will take the necessary action ie: report to the Portal.
- The School ensures that the use of Internet derived materials by staff and by pupils complies with copyright law.

Managing Internet access:

- The security of the school information systems will be reviewed regularly.
    - The technical infrastructure is secure – support is provided by Turn-it-On
    - Users are only able to access networks and devices by using a password

- Virus protection is installed and updated regularly.
- The school uses EXA broadband through Turn It On and Sophos Antivirus through Oxfordshire County Council.
- Portable media should not be used without specific permission and a virus check.
- Unapproved systems utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.

Email:

- Staff are advised to use their school email addresses for any school related correspondence but to be aware that this is not a secure system. Passwords should be considered for documents that contain sensitive information.
- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal email accounts may be blocked.
- Social emailing interferes with learning and is restricted.
- The forwarding of chain letters is not permitted.

Published content and the school website:

- The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information is not be published.
- Email addresses are generally not published, to avoid spam harvesting. Contact forms are used where possible.
- The Headteacher takes overall editorial responsibility and ensure that content is accurate and appropriate.
- The website complies with the school's guidelines for publications including respect for intellectual property rights and copyright.

Publishing staff and pupil's images and work:

- Photographs that include pupils are selected carefully and do not enable individual pupils to be clearly identified by name.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Parents or carers are asked each September to notify the school, in writing, if they give permission for the school to use their child's photograph in school publications (which includes the school website).
- Images of staff are not published without consent from that member of staff.

Social networking and personal publishing:

- Social networking sites and news groups are blocked unless a specific use is approved.
- Pupils are advised not to, and educated about the risks of, signing up to any social networking site that is not age appropriate. eg. Facebook
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline telephone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They are educated to consider how public the information is and when and how to use private areas. Advice is given regarding background detail in a photograph which could identify a pupil or his/her location eg: house number, street name, school or shopping centre.

- Staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of any images.
- Pupils are advised and educated about security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students are encouraged to invite known friends only and deny access to others.
- Pupils are advised not to publish specific and detailed private thoughts.
- The School is aware that bullying can take place through online activity, in particular social networking, especially when a space has been setup without a password and others are invited to see the bully's comments.
- See "Acceptable Use of ICT Policy" for further information relating to staff use of social networking.

Technical infrastructure/equipment, filtering and monitoring:

- The school uses Turn-It-On to support the management of its computer equipment and systems including the network and internet access
- The school ensures filtering systems are as effective as possible in collaboration with ICT technical support.
- Any material that the school believes is illegal is reported to appropriate agencies such as :
  - Internet Watch Foundation (IWF) : www.iwf.org.uk or
  - Child Exploitation and Online Protection Centre (CEOP) : www.ceop.police.uk
  - If appropriate, the Local Authority Designated Officer for Safeguarding (LADO)
- Servers, wireless systems and cabling areEXA securely located and physical access is restricted
- Users have clearly defined access rights to the school's technical systems and devices
- All users, including KS2 pupils, have username and password access to the school network
- The School Business Manager is responsible for ensuring that software licence logs are accurate and up to date
- There is a 'guest' system in place for temporary users of the school network
- There is an Acceptable Use of ICT policy which all staff and volunteers must adhere to

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.

Protecting personal data:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school ensures that it holds the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained and lawfully processed
- The school has a data protection policy
- The school is registered as a Data Controller for the purposes of the Data Protection Act
- Staff ensure that they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Staff use personal data only on secure password protected computers and other devices ensuring they are properly logged off at the end of any session in which they are using personal data
- Transfer data using password protection where possible

Authorising Internet access:

- The school maintains a record of all staff and pupils who are prohibited Internet access.

- All users must read and abide by the rules as detailed in the school's "Guide to staying safe on the internet" before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents of all children are provided annually with a "parents' guide to keeping children safe on the internet"

Assessing risks:

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school takes *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 Oxfordshire County Council can accept liability for the material accessed, or any consequences of Internet access.
- The Headteacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.
- 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 are reviewed regularly.

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 who should use the agreed Oxfordshire County Council procedures.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Introducing online safety to pupils:

- Copies of the 'Pupil's online safety agreement' are posted in all networked rooms, including classrooms.
- Pupils are informed that Internet use is monitored.
- Online access is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. Online safety education is broad and relevant with progression related to the age and development of pupils. This follows the 'Education for a Connected World' framework.
- Instruction in responsible and safe use precedes all Internet access.
- A planned online safety curriculum is provided as part of the curriculum but, as detailed above, is revisited regularly across the whole curriculum.
- Online safety messages and procedures are reinforced through assemblies, anti-bullying work and safety week.

This policy supports and complements Hill View's Safeguarding policy to ensure the school takes all necessary steps to protect the welfare of all children in our care.