Hope View School

Online Safety Policy

Introduction

The school's Online Safety Coordinators are Mrs C Lorne (Headteacher) and Mr Alex Napier (Network Manager)

The leader governor for Safeguarding is Mr David Hillier

Our Online Safety Policy has been written by the school, with reference to the Kent Online Safety Policy and government guidance.

Date of Policy: August 2018
Policy Review Date: August 2019

Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.
- 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.
- 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 access is an entitlement for students who show a responsible and mature approach to its use

How does internet use benefit education?

- Benefits of using the internet in education include:

- Access to world wide educational resources
- Access to learning and wherever and whenever convenient,
- Educational and cultural exchanges between pupils world-wide.
- Professional development for staff through access to national developments, educational materials and effective classroom practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration dates with Medway and Kent County council and DFE.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils to enhance and extend education. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.
- Staff should guide pupils to Online Safety 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
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The evaluation of Online Safety materials is part of teaching/learning in every subject.

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Managing Internet Access
Information system security

- School ICT systems security is updated automatically on a daily basis and will be reviewed by the ICT Subject Leader as required, but especially when new equipment and programmes are purchased.
- Virus protection will be updated automatically.
- Workstations are secured against user mistakes and deliberate actions.
- The server is located securely and physical access is restricted. The server operating system is secured and kept up to date.
- Access by wireless devices are pro-actively managed.
- Security strategies will be discussed with the Proprietors.
- Users must act responsibly e.g. downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.

E-mail

Pupils may only use approved e-mail accounts on the school system.

- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Staff should only use the main school email account to communicate with pupils as approved by the senior Leadership team.
- Access in school to external personal e-mail accounts may be blocked.

Published content and the school web site

- Staff or pupil personal contact information will not be published.
- The contact details on the website are the school address, email and telephone
- number.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other Online Safety space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Examples would include real name,

address, mobile or landline phone numbers, school attended, e-mail addresses, full names of family/friends, specific interests and clubs.

- Pupils will advised not to place personal photos on any social network space.
- Advice will be given regarding background detail in a photograph which could identify the student or his/her location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for pupils of all ages.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff should not run social network spaces for pupil use on a personal basis.
- Pupils and staff are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff are not to make contact or accept requests from pupils who attend or have previously attended the school under any circumstances.

Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator and/or the Network Manager.
- Senior staff will ensure that annual checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF(internet watch foundation) or CEOP.

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.
- The senior leadership team should note that technologies such as mobilephones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones must be handed in by all pupils upon arrival in the school each morning. Any pupil who does not adhere to this rule risks having their phone confiscated.

- Games machines including the Microsoft Xbox will not be connected to the Internet on any occasion. Care is required in any use in school or other officially sanctioned location. Pupils may only plan age appropriate games and must be supervised by a member of staff.
- Staff will be issued with a school phone where contact with pupils is required or where mobile phones or iPads are used to capture photographs of pupils.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read and sign the "Staff Acceptable Use Policy for ICT" before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Throughout the school, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use on an annual basis to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

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 head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures. (The Kent Online Safety Policy has a flowchart of responses to an incident of concern.)
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet or the school network.
- All Online Safety complaints and incidents will be recorded by the school – including any actions taken.
- Discussions will be held with the Police Safer Schools Partnership Coordinators and/or children's safeguards unit to establish procedures for handling potentially illegal issues.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to Online Safety.
- The school will be sensitive to internet related issues experienced by pupils out of school. E.g. social networking sites, and offer appropriate advice.

How will cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the schools policy on anti-bullying.
- There will be clear procedures in place to support anyone affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyberbullying may include:
- The bully will be asked to remove any material deemed to be inappropriate or offensive
- Service provider may be contacted to remove content.

- Internet access may be suspended at school for the user for a period of time.
- Parent/carer may be informed.
- The police will be consulted if a criminal offence is suspected.

Communications Policy

Introducing the Online Safety policy to pupils

- Online Safety rules will be posted in all rooms where computers are used and discussed with pupils at the beginning of each academic year, with reminders each time they use the ICT suite or computers in classrooms.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in Online Safety will be developed to raise the awareness and importance of safe and responsible internet use.
- Online Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHEE) curriculum covering both safe school and home use

Staff and the Online Safety policy

All staff will be given the School Online Safety Policy and its importance explained.

- To protect all staff and pupils, the school will implement acceptable use policies.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.
- Staff training in safe and responsible internet use both professionally and personally will be provided.

Enlisting parents’ and carers’ support

- Parents_ and carers_ attention will be drawn to the School Online Safety Policy in
- Newsletters and on the school Web site.
- The school will maintain a list of Online Safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil acceptable use agreement when they register their child with the school.

- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.

Equality and Diversity

Hope View School is committed to equality of opportunity for all pupils and staff in which people treat each other with mutual respect, regardless of: age, disability, family responsibility, marital status, race, colour, ethnicity, nationality, religion or belief, gender, gender identity, transgender, sexual orientation, trade union activity or unrelated criminal convictions. We strive to educate, promote and celebrate the wider diversity of society within our school community.

Related Policies:

Safeguarding Policy

Behaviour and DisciplinePolicy

Rewards and Sanctions Policy

Anti Bullying Policy

Policy Review Date: August 2019

Responsible Person: Mrs C Lorne

Appendix 1: Possible Teaching and Learning Activities
See separate sheet.

Appendix 2: Useful resources for teachers
Please refer to the DFE's Online Safety policy guidance for further information.
BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Becta
http://schools.becta.org.uk/index.php?section=is
Chat Danger
www.chatdanger.com/
Child Exploitation and Online Safety Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kent Online Safety Policy and Guidance, Posters etc.
www.clusterweb.org.uk/kcn/Online Safety_home.cfm
Kidsmart
www.kidsmart.org.uk/
Kent Police – Online Safety
www.kent.police.uk/Advice/Internet%20Safety/Online Safety%20for%20teacher.html
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents
Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD
http://publications.teachernet.gov.uk
Family Online Safety Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Kent leaflet for parents: Children, ICT & Online Safety
www.kented.org.uk/ngfl/ict/safety.htm
Parents Centre
www.parentscentre.gov.uk
Internet Safety Zone
www.internetsafetyzone.com