Hawridge and Cholesbury CE School

School E-Safety Policy

Date: January 2019

Review Date: January 2021

Contents

Contents 2
Members of staff responsible: 10
1 Writing and reviewing the e-safety policy 3
2 Teaching and learning 3
2.1 Why the Internet and digital communications are important 3
2.2 Internet use will enhance learning 3
2.3 How internet use benefits the learning of pupils and staff 3
2.4 Pupils will be taught how to evaluate Internet content 4
3 Managing Internet Usage 4
3.1 Published content and the school web site 4
3.2 Publishing pupils' images 4
3.3 Pupil Social networking and personal publishing 4
3.4 Staff Social networking and personal publishing 5
3.5 E-mail and Pupils 5
3.6 E-mail and Staff 5
4 Managing Internet Access 6
4.1 Managing filtering 6
4.2 Managing mobile phone use by pupils 6
4.3 Managing mobile phone use by staff 6
4.4 Managing pupils taking digital photographs of staff 6
4.4 Managing staff photographing pupils 6
4.5 Managing parent photographs of pupils and staff 6
4.6 Managing videoconferencing & webcam use 7
4.7 Managing new technologies 7
5 Protection of information 7
5.1 Protecting personal data 7
5.2 Protecting School Data 7
5.3 Information system security 7
6 Policy Decisions 8
6.1 Authorising Internet access 8
6.2 Assessing risks 8
6.3 Handling e-safety complaints 8
6.4 Management of Cyberbullying within school 8
6.5 Management of any issues arising, from internet use, outside of school 9
7 Communications Policy 9
7.1 Introducing the e-safety policy to pupils 9
7.2 Staff and the e-Safety policy 9
7.3 Enlisting parents' and carers' support 9
Appendix 1: Hawridge & Cholesbury Pupil and Parent e-Safety Code of Practice 11
Appendix 2 Useful resources for teachers 13
Appendix 3: Useful resources for parents 13

1 Writing and reviewing the e-safety policy

Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors.

The Computing Co-ordinator is the E-Safety Co-ordinator. They will work closely with the Designated Safe-guarding Lead {DSL] as the roles overlap. It is not a technical role.

2 Teaching and learning

2.1 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 pupils who show a responsible and mature approach to its use.

2.2 Internet use will enhance learning

The school Internet access is designed expressly for pupil use and includes filtering by the service provider appropriate to the age of pupils.

- Pupils will be taught, at the start of each year, what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will also be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.3 How internet use benefits the learning of pupils and staff

Benefits of using the internet in education include:

- Access to worldwide educational resources.
- Access to online search engines for research.
- Access to online programming and curriculum student resources.
- Access to learning 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 data with Bucks County Council.

2.4 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials is evaluated before its use 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 both within school and at home. 'Unpleasant' is deemed to be anything that makes the child feel uncomfortable or which they feel is inappropriate.
- Key Stage 2 children will increasingly be encouraged to reflect upon the suitability and appropriateness of web sites for their age, both in terms of search results and in online social networks e.g. FaceBook.

3 Managing Internet Usage

3.1 Published content and the school web site

- The contact details given online should be the school's only. Staff personal contact information will not be published.
- The Headteacher and the school's website manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.2 Publishing pupils' images

- Written permission from parents or carers will be obtained on entry to the school and kept on file before photographs of pupils are published on the school website.
- Photographs that include pupils will be selected carefully, so that individual pupils cannot be identified or their image misused. Wherever possible, group photographs rather than full-face photos of individual children will be used. The only exception to this is when photos are to be used for a specific purpose e.g. a school poster, in which case parental approval would be obtained prior to the image being used.
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic devices.
- Staff are not permitted to publish any pupil images, other than through the school website.

3.3 Pupil Social networking and personal publishing

- The school will not allow use of social networking sites.
- Children will be made aware that social networking sites have age restrictions and should be informed not to lie about their age on these sites.
- In PSHE and e-Safety lessons, pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. They will also learn about the importance of using gender neutral user names.
- Pupils will also be advised on providing photographs online, both in terms of a background, which could identify the pupil's location or school, and in terms of the loss of ownership once it is uploaded online.
- Upper Key Stage 2 children will also be made aware of and advised against placing inappropriate images of themselves online. Sexting is an issue which the Year 6 children will discuss as part of the Sex and Relationship Education [SRE] teaching.

- Through the CEOP site, pupils will be made aware of the potential risks of social networking and chat-rooms.
- The school is aware that bullying can take place through these social networking sites and any such instances will be dealt with in accordance with the School's Bullying Policy.
- Parents are to be updated, as often as possible, of the changing nature of social media sites, recommendations made by CEOP and other organisations such as Parent Zone. The aim being to ensure pupil use of these sites is monitored and controlled outside of school, as well as inside.

3.4 Staff Social networking and personal publishing

- Staff are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff will adhere to the rule that any friend request from a child in their school must NOT be accepted. Equally, no staff should request friendship with a current pupil.
- The school name and images should not be used on social networking sites or web pages without the prior permission of the Head teacher and/or Governing Body.
- It is recommended that staff do not accept friend requests from existing parents. Whilst it is understood that certain members of staff are also parents, who therefore might have other parents as friends on social media, they are asked to be mindful of this when posting
- Staff should also regularly check their privacy settings both to control who can see their posts and also to ascertain what information is visible, should their name be used in a search engine.

3.5 E-mail and Pupils

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In any e-mail communication, pupils must not reveal either their personal details or those of others, nor should they arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- E-mail sent from pupils to external bodies is to be reviewed by the teacher and authorised by them before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain letters is not permitted.

3.6 E-mail and Staff

- Staff are only to use their work based Bucksgfl address, both within school and for communicating with other staff.
- Staff may only initiate contact with children for professional reasons, for example in the teaching of email-based aspects of the Computing curriculum.
- Staff should not initiate any personal correspondence with pupils and if they receive an email from a pupil, outside of school based curricular work, a simple acknowledgement will be sent, with no encouragement to continue the dialogue.

4 Managing Internet Access

4.1 Managing filtering

- The school will work with the Bucks County and the School's technical support organisation, WiBird, to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils encounter unsuitable on-line materials, the site must be reported to the e-Safety Co-ordinator or the Headteacher, in her role DSL
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

4.2 Managing mobile phone use by pupils

- On a normal, day-to-day-basis, pupils are not allowed to have mobile phones within school.
- In special circumstances, notified to the school by the parent, a pupil may bring a mobile phone to school but it must be switched off and handed in to the office upon arrival. The mobile is then to be collected at the end of the day and only switched on once the pupil has left the school premises.
- Any mobile phone discovered in the possession of a pupil in school will be immediately switched off and removed. The phone will be kept in the school safe and returned directly to the child's parent or carer at the end of the day.

4.3 Managing mobile phone use by staff

- No mobile phones are to be visible or be used by staff during lesson time. They should be stored safely away in either one of the lockers provided or in the classroom cupboard.
- Where contact with the school is required on a school trip or when the member of staff is off school premises, for example on the Common, staff must either take the school mobile phone or their own, provided that their phone number is given to the office staff.

4.4 Managing pupils taking digital photographs of staff

No digital cameras are permitted on any school trips.

4.4 Managing staff photographing pupils

- Photographs taken by staff to support pupil learning or as a record of school events and trips, e.g. Kith and Kin Days, visits to Museums, should only be taken using school digital cameras or tablets.
- Images can only be downloaded onto the school server and at no time can they be stored on home-based laptops or computers.
- All printing of pupil images by staff must be done on school printers. No images should be sent to a third party for printing.

4.5 Managing parent photographs of pupils and staff

- Parents are to sign their section of the Pupil and Parent e-Safety Code of Practice (see Appendix 1) which covers the taking of photos and videos.

- For internal school events, e.g. the Key Stage 1 Nativity and the Key Stage 2 End of Year Production, parents and carers are to be reminded that all photographs and videos containing images of children (other than their own) or staff, are not to be shared on any form of social media.

4.6 Managing videoconferencing & webcam use

- Videoconferencing should use the school's WiFi to ensure security.
- Videoconferencing and webcam use will be appropriately assessed by staff as being relevant and appropriate for the pupils' age.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- School videoconferencing equipment should not be taken off school premises without permission.
- Videoconferencing contact information should not be put on the schools website.
- Parents and carers should agree for their children to take part in videoconferences.
- When recording a videoconference lesson, written permission should be given by all sites and participants.

4.7 Managing new technologies

- Emerging technologies will be examined for educational benefit by the Computing Co-ordinator.

5 Protection of information

5.1 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

5.2 Protecting School Data

- Staff are only permitted to use the encrypted memory stick provided by the school.

5.3 Information system security

- School computing systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the IT provider.
- In line with the GDPR, pupil data sent over the Internet will be encrypted or otherwise secured.

6 Policy Decisions

6.1 Authorising Internet access

- All staff must read and sign the 'Code of Conduct, which includes e-safety for Computing' before using any school computing resource
- Parents will be asked to read with their child, sign and return an e-Safety Code of Practice form upon entry to the school. They will also be asked to sign the parent section of the same document.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign an 'Acceptable use of school computing resources' before being allowed to access the internet from the school site.

6.2 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. Neither the school nor the broadband provider can accept liability for any material accessed, or any consequences of Internet access.

- The school will audit computing use to establish if the e-Safety Policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

6.3 Handling e-safety complaints

- Complaints of Internet misuse by pupils or staff will be dealt in accordance with the school's Complaints Policy or the Whistle Blowing Policy (whichever is appropriate).
- Pupils and parents will be informed of the consequences for pupils misusing the Internet. These would depend upon the severity of the misuse but would automatically result in the child not having access to the Internet until the matter was discussed by all parties concerned.

6.4 Management of Cyberbullying within school

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Should an instance occur, the following will take place:

- Support would be given for anyone affected by cyberbullying.
- 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 if necessary.
- Appropriate sanctions for those involved in cyberbullying would come into immediate affect whilst the above steps are being taken. This may include the removal of any material deemed to be inappropriate or offensive, the suspension of Internet access in school for a given period of time.
- The Parent or Carer will be informed and an initial meeting held with the Headteacher and the class teacher to discuss the allegation of cyberbullying, the steps being taken and the consequences for their child.

6.5 Management of any issues arising, from internet use, outside of school

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites and offer appropriate advice.

7 Communications Policy

7.1 Introducing the e-safety policy to pupils

- e-Safety rules will be discussed with all pupils at the start of each academic year and with regular reminders.
- e-safety posters are to be displayed around the school.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- e-Safety training will be embedded within both the Computing scheme of work and the Personal Social and Health Education (PSHE) curriculum.

7.2 Staff and the e-Safety policy

- All staff will be instructed to read the School e-Safety Policy and sign to say that they have done so.
- All staff are to sign the Staff Code of Conduct
- Staff should be aware 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 computing use will be supervised by the Headteacher and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.
- Any websites or web content that needs blocking can be done by using the adblock symbol in the top right hand corner of the screen.

7.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.
- The school will include on its website, resources available to inform and guide parents.
- The school will ask all new parents to sign the Pupil and Parent e-Safety Code of Practice when their child joins the school.

The public sector equality duty of the Equality Act 2010 has been considered in the writing of this policy. A Discrimination Impact Assessment concludes that through this policy Hawridge & Cholesbury C of E School seeks to:

- Eliminate discrimination, harassment and victimisation and other conduct prohibited by the Act.
- Advance equality of opportunity between people who share a protected characteristic and those who do not.
- Foster good relations between people who share a protected characteristic and those who do not.

Protected Characteristics: age, disability, gender, gender identity, race, religion or belief, and sexual orientation.

Members of staff responsible:

Headteacher

- **The e-Safety Policy was revised by:** Jude Kretschmer
- **It was approved by the Governors on:** 16th January 2019
- **The next review date is: January 2021**

Appendix 1: Hawridge & Cholesbury Pupil and Parent e-Safety Code of Practice

As a pupil of Hawridge & Cholesbury:

- I will only use the internet when supervised by a teacher or adult.
- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- I will never send anyone my picture without permission from my teacher/parents/carer.
- I will never give my password to anyone, even my best friend, and I will log off when I have finished using the computer.
- I will never arrange to meet anyone in person without first agreeing it with my parents/teacher/carer and get them to come along to the first meeting.
- I will never hang around in an Internet chat room if someone says or writes something which makes me feel uncomfortable or worried, and I will always report it to a teacher or parent.
- I will never respond to unpleasant, suggestive or bullying e-mails or bulletin boards and I will always report it to a teacher or parent.
- I will not look for bad language or distasteful images while I am online and I will report bad language or distasteful images to a teacher or parent if I come across them accidentally.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I know that my teacher and the Internet service provider will check the sites I have visited!
- I understand that I can access only sites and material relevant to my work in school and that I will not be able to use the Internet if I deliberately look at unsuitable material.
- I understand that I will not be able to use the Internet if I deliberately hack into the schools' or other systems.
- I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I know that the contents of my e-mail messages will be monitored by the Computing Co-ordinator.
- I may not download software from the Internet (including screen savers, games, video clips, audio clips, *.exe files).
- I know that information on the Internet may not always be reliable and sources may need checking. Web sites may be sponsored by advertisers.

- I will not use e-mail to send or encourage material which is pornographic, illegal, offensive or annoying or invades another person's privacy

As a parent of a child who is a pupil at Hawridge & Cholesbury School:

- I will help my child to follow the e-Safety code of practice.

- I will not share on social media any digital photos of staff or of children, other than my own.

Pupil's Name.....

I have read the Pupil and Parent e-Safety Code of Practice and I have discussed it with my son/daughter/ward. We agree to support the school's e-Safety Policy.

Printed name
(Parent/Guardian/Carer)……..

Signed ……

Date ……

Appendix 2 Useful resources for teachers

Child Exploitation and Online Protection Centre www.ceop.gov.uk/

Childnet https://www.childnet.com/

Cyber Café http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen http://www.digizen.org/

Bucks e-Safety Policy and Guidance, Posters etc

Think U Know www.thinkuknow.co.uk/

UK Council for Internet Safety www.gov.uk/government/organisations/uk-council-for-internet-safety

Appendix 3: Useful resources for parents

Parent zone https://parentzone.org.uk/home

Childnet https://www.childnet.com/

Family Online Safe Institute www.fosi.org

Internet Watch Foundation www.iwf.org.uk

Internet Safety Zone www.internetsafetyzone.com