Online Safety Policy

Knaphill Federation of Schools	
Policy: Online Safety	
Governors' Committee Responsible:	
Policy Originator: L Fini	**Review Period:** 3 years
Status: Statutory	**Next review Date:** Spring 2020

The Knaphill Federation of Schools Online Safety Policy

Internet safety is part of our school's safeguarding responsibilities. The Online Safety Policy relates to other policies, including those for Computing, anti-bullying, behaviour and for child protection.

The Computing leader is also the Internet Safety leader.

Using this policy:

- The schools will form an Internet Safety committee and will appoint an Internet Safety Leader.
- The schools have written our Online Safety Policy; it builds on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The Online Safety Policy was revised on: September 2017.
- The Governors approved the Online Safety Policy on: _____.
- The Online Safety Policy and its implementation will be reviewed annually. The next review is due on: Autumn 2018.
- The Online Safety Policy covers the use of all technology that can access the school network and the Internet, or which facilitates electronic communication from school beyond the bounds of the school site.
- The Online Safety Policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Teaching and Learning

Internet and Digital Communications

- The Internet is an essential element in the 21st century life for education, businesses and social interaction. The school has a duty to provide students 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.
- The school filtering service is provided by Smoothwall, which includes filtering appropriate to the age of pupils and provides daily reports to the DSL.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the safe, effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- Pupils are educated on how to stay safe online outside of school through our Internet safety lessons and workshops, this includes social media.
- Parents are educated on how to keep their children safe online through external visitors and regular updates are sent home.

Pupils will be taught how to evaluate Internet content

- Our schools will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials that they read and shown how to validate 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. For pupils whose parents lack economic or cultural educational resources, the school will build digital skills and resilience, acknowledging the lack of experience and Internet at home. For children with social, or psychological vulnerabilities, further consideration will be taken to reduce potential harm.

Managing Internet Access

Our schools will provide managed Internet access to its staff and pupils in order to help pupils learn how to assess and manage risk; to gain the knowledge and understanding to keep themselves safe when using the Internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will ensure that all Internet access has age appropriate filtering provided by a recognised filtering system, which is regularly checked to ensure that it is working, effective and reasonable.
- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- The school recognises the changes to HTML websites and has put certificates in place to ensure the safety of the pupils
- The school will ensure that its networks have virus and anti-spam protection and will ensure that this is updated regularly.
- Access to school networks will be controlled by personal passwords.
- Systems are in place to ensure that Internet use is monitored and a log of any incidents is kept to help identify patterns of behaviour and to inform the Online Safety policy.
- The school computing systems will be reviewed regularly.
- All staff that manage filtering systems, or monitor computing use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the Internet via school equipment for anyone who is not employed by the school is filtered and monitored.

Internet Use

Our school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe; how to protect themselves from harm and how to take responsibility for their own and others' safety. This will be taught across all year groups. All communication between staff and pupils, or families will take place using school equipment and/or school accounts. Pupils will be advised not to give out personal details or information that may identify them or their location. At the Knaphill Federation of Schools, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Email

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

- Staff to pupil e-mail communication must only take place via a school email address and must be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves, or others in e-mail communication, or arrange to meet anyone without specific permission.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published Content and the School Website

- The contact details on the School Website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that the content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will be avoided on the website or learning platform including blogs, forums or wikis, particularly in association with photographs.
- Written permission will be obtained from parents, or carers before photographs of pupils are published on the school website.
- 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 on the School Learning Platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Newsgroups will be blocked unless specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of opportunities, however, it does present dangers for primary and secondary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing Filtering

- If staff or pupils come across unsuitable online materials, the site must be reported to the Internet Safety co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A log of any incidents may be useful to identify patterns and behaviours of the pupils.

Managing Video Conferencing

- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff.
- Pupils must ask permission from a member of staff before making or answering a video call.

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.
- Staff will use a school phone where contact with pupils is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.
- The school cannot be held responsible for the loss or damage of any personal devices used in school, or for school business.
- Staff must not store images of pupils, or pupil personal data on personal devices.
- Personal equipment may be used by staff to access the school IT systems, provided their use complies with the Online Safety policy and the relevant AUP.

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 (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, computing technicians and governors) must read and sign the 'Staff AUP' before accessing the school computing systems.
- The school will maintain a current record of all staff and pupils who are granted access to school computing systems.
- People not employed by the school must read and sign a Guest AUP before being given access to the Internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

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. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- Our school will monitor computing use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.
- Any pupils suspected of trying to access inappropriate material, for example, extremist material or pornography will be dealt with by the safeguarding procedures.

Handling Online Safety Risks

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the Internet and this will be in line with the schools' behavior policy.
- Any complaint about staff misuse must be referred to the head teacher.
- Pupils and parents will be informed of the complaints procedure.

Community of the Internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school Online Safety policy.

Communication of the Policy

Introducing the Online Safety policy to pupils

- Appropriate elements of the Online Safety policy will be shared with pupils.
- Online safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of Internet safety issues and how best to deal with them will be provided for pupils. This should be addressed each year as students become more mature and the nature of newer risks can be identified.
- Pupils need to agree to comply with the pupil AUP in order to gain access to the school Computing systems and to the Internet.
- Pupils will be reminded about the contents of the AUP as part of their Internet safety education

Staff and the Online Safety policy

- All staff will be shown where to access the Online Safety policy and its importance explained.
- All staff must sign and agree to comply with the Online Safety policy in order to gain access to the school computing systems and to the Internet.
- All staff will receive online safety training.

Enlisting parents' support

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school web site.
- Parents will be informed on Internet safety and have an overview of tools to allow them to take control whilst not undermining trust.
- Parents are regularly invited into school for online safety talks and any updates on Internet safety are provided through our school newsletter and website.

Appendix 1

Staff, Governor and Visitors
Acceptable Use Policy / Computing Code of Conduct

The Knaphill Federation of Schools
Computing and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of computing. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher.

- I appreciate that computing includes a wide range of systems, including mobile phones, iPads, Learn Pads, digital cameras, email, social networking.
- I understand that mobile phones or any personal device cannot be used around the children. The only exception if an emergency call is needed to be made on an off-site school trip.
- I understand that it is a criminal offence to use a school computing system for a purpose not permitted by its owner.
- I will comply with the computing system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not install any hardware or software without the permission of the headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that all my use of the Internet is monitored and logged and can be made available, on request, to my Head teacher.
- I will respect copyright and intellectual property rights.
- Images of pupils and/or staff will only be taken using a school device, stored and used for professional purposes in line with school policy. Written consent of the parent or carer will be obtained. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head teacher.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will ensure that all electronic communications with parents, pupils and staff, including email and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's Online Safety policy and help pupils to be safe and responsible in their use of computing and related technologies. I will promote Internet safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the Internet safety Coordinator, the Designated Safeguarding Lead (DSL) or Headteacher.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serous infringements may be referred to the police.

I agree to follow this code of conduct and to support the safe use of computing throughout the school.

Full Name…… (Printed)

Job title…… Signature…… Date……

Appendix 2

Knaphill Junior School's Online Safety Rules

Acceptable use of the school computers

These rules will help to keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework
- I will ask permission before using the school's computers
- I will only login to the school systems as myself
- I will only edit or delete my own files
- I am aware that some websites and social networks have age restrictions which mean that I should not go on them
- I will only visit internet sites that a responsible adult has approved
- I will immediately close any webpage that I am not sure about
- I will only communicate with people I know, or that a responsible adult has approved

- I will not open an attachment, or download a file, unless I have been given permission by an adult
- I will not tell anyone my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- If I see anything I am unhappy with or I receive a message I do not like, I will show a responsible adult.

Appendix 3

Online Safety Rules and Sanctions

It is appropriate for people to be allowed a great deal of freedom in using computing for study, work and leisure. With freedom comes responsibility. The Knaphill Federation of Schools cannot control what people, all over the world, make available on the Internet; a small proportion of the material which it is possible to access is not acceptable in school, whilst other material must be treated with great sensitivity and care. Exactly the same standards apply to electronic material, as to material in any other form. If material is considered to be unacceptable by the school when presented in a book, magazine, video, audio tape or spoken form, then it is not acceptable on the computing network.

We expect all computing users to take responsibility in the following ways:

- Not to access or even try to access any material which is:
- Violent or that which glorifies violence
- Criminal, terrorist or glorified criminal activity (including drug abuse)
- Racist or designed to incite racial hatred
- Of extreme political opinion
- Pornographic or with otherwise unsuitable sexual content
- Crude, profane or with otherwise unsuitable language
- Blasphemous or mocking of religious and moral beliefs and values
- In breach of the law, including copyright law, data protection, and computer misuse
- Belongs to other users of computing systems and which they do not have explicit permission to use
- Not to search for, or use websites that bypass the school's internet filtering
- Not to download or even try to download any software without the explicit permission of the headteacher
- Not to attempt to install unauthorised and unlicensed software
- To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number to strangers
- Not to use other people's user ID or password, even with their permission
- Not to interfere with or cause malicious damage to the computing Facilities
- To report any breach (deliberate or accidental) of this policy to the headteacher immediately.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. The Knaphill Federation of Schools reserves the right to access all material stored on its computing system, including that held in personal areas of staff and pupil accounts for purposes of ensuring DfE, Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who is found not to be acting responsibly in this way will be disciplined. Irresponsible users will be denied access to the computing facilities. Knaphill School will act strongly against anyone whose use of computing risks bringing the school into disrepute or risks the proper work of other users. Persistent offenders will be denied access to the computing facilities – on a permanent basis.

Appendix 4

Use of Digital Images

To comply with the Data Protection Act 1998, we need parental permission to use photographs or recordings of any child. When posting images for external use, we will avoid using surnames.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
Only images of pupils in suitable dress will be used.

Staff are not allowed to take photographs or videos on their personal equipment.

There are many opportunities for digital imagery to be used, for example, during a learning activity to demonstrate or evaluate work, to present work to others, to share good practise with the wider community, to celebrate achievements and many more.

These may be displayed on our **website**, which is public facing and could potentially be viewed by anyone on the internet, or they may be displayed on our **virtual learning environment**, which is private to the school community and can only be viewed by those with a username and password.

We would like to ask your permission for

Use of digital images - photography and video:

I agree to the school using photographs or videos of my child _____ (name)

On the public facing website: **yes / no** (please circle)

I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature: _____

Date: ___/___/___

Appendix 5

Online Safety Agreement

Parent/Guardian Consent Form and Online Safety Rules

All pupils use computer facilities, including Internet access, as an essential part of learning at Knaphill School, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the Internet safety rules have been understood and agreed.

Parent/Guardian Name: _____

Pupil Name: _____

- As the parent or legal guardian of the above pupil, I have read and understood the attached school Internet safety rules and grant permission for my daughter or son to have access to use the Internet and other Computing facilities at school.

- I know that my daughter or son has signed an online safety agreement form and that they have a copy of the online safety rules. We have discussed this document and my daughter or son agrees to follow the online safety rules and to support the safe and responsible use of Computing at Knaphill School.

- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, employing appropriate teaching practice and teaching online safety skills to pupils.

- I understand that the school can check my child's computer files and the Internet sites that they visit and that if they have concerns about their online safety or behaviour they will contact me.

- I understand the school is not liable for any damages arising from my child's use of the Internet facilities.

- I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/Guardian Signature: _____

Date: ___/___/___

A full copy of the school's Online Safety policy is available on the school website.