KING'S WOOD SCHOOL AND NURSERY

E-SAFETY POLICY

<u>On-line Safety</u>

The use of technology has become a significant component of many safeguarding issues. As a school we seek to protect and educate our pupils and escalate any incident where appropriate. We work with pupils around the three areas of risk – content, contact and conduct; giving them the skills and knowledge to help them to stay safe on-line.

<u>Creating a safer online environment</u>

As a school we do all that we reasonably can to limit children's exposure to on-line risks. The school uses the Bucks County system as our network provider. This is managed by Up-Data who ensure our firewalls are strong and any inappropriate content does not get through. If inappropriate websites are accessed an alert is issued which the school technician can follow up on.

Children are unable to access any social media websites through the school's system. The schools IT technician and Soft Egg monitor the system and review usage.

<u>Safe and responsible use</u>

Giving everyone the skills, knowledge and understanding to help children and young people stay safe on line is vital. The guidelines for children and staff in this policy and our use of social media policy clearly outline our expectations with regard to internet use.

Computing and PSHE lessons will frequently include information around keeping safe and it is often the topic of assemblies. Parents' sessions are also offered on a regular basis. Our school website contains a section on e-safety with links to helpful sites. The school also uses CEOPs as a resource to inform and educate.

Events such as anti-bullying week will always have a focus on the effects of cyber-bullying and our PSHE curriculum regularly covers internet use with a focus on pupils' rights and responsibilities.

<u>Social Media and Camera equipment</u>

The school's social media policy provides clear guidance on acceptable use, as does the staff Code of Conduct. Use of mobile phones and camera equipment are also covered in the Code of Conduct. Children are expected to hand mobile phones into the office when they arrive in school and collect them at the end of the day.

<u>Concerns</u>

Any concerns over internet use should be reported to the designated safeguarding lead, the headteacher. If she is not available one of the four deputy DSLs should be told. The incident should then be logged on CPOMS.

Alternatively staff can contact the BCC safe-guarding team for advice. Severe incidents may require contacting the police.

Reviewed: February 2020

The school provides computers (***1**) for use by students. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as USBs, flash drives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.

Security and Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number, your school's name, or send them your picture, unless you are given permission to do so.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Staff may review files and communications to ensure that users are using the system responsibly.

Internet

- Do not access the Internet unless for study or for school authorised / supervised activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet.
- Never arrange to meet anyone unless your parent/guardian or teacher goes with you. People you contact online are not always who they seem.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff.

*1 - Throughout this policy the term computers also refers to I-Pads

Reviewed: February 2020

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If any student violates these provisions, access to the Internet will be denied and the student will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

Pupils' Internet Code of Practice – King's Wood School and Nursery

- 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 use an Internet chat room.

- 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/carer.

- I will not look for bad language or distasteful images while I'm 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 Network Manager

- 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 illegal, offensive, annoying or invades another person's privacy

I have read the Pupils' Code of Practice and I have discussed it with my son/daughter/ward. We agree to support the school's policy on the use of the Internet

Signed (Parent/Carer) …………………………Pupil ……………..................Date ……………. **Pupil Name ....**

The school provides computers (***1**) for use by teachers. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all teachers, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install, or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as memory sticks, USBs, flash drives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.

Security & Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- IT staff may review files and communications to ensure that users are using the system responsibly.

Internet

- Do not access the Internet unless for school activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, extremist or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet using school computers.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of ICT staff.

*1 - Throughout this policy the term computers also refers to I-Pads

Reviewed: February 2020

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If any teacher violates these provisions, access to the Internet will be denied and the teacher will be subject to disciplinary action.

Teacher's Internet Code of Practice

- Teachers should be familiar with the school's Network, Internet, e-mail and web site creation policies and the pupils' code of practice for Internet use.

- Teachers should closely monitor and scrutinise what their pupils are accessing on the internet including checking the history of pages.

- Computer monitor screens should be readily visible for the teacher, so they can monitor what the pupils are accessing.

- Pupils should have clear guidelines for the content of e-mail messages, sending and receiving procedures.

- Use of the Internet should be supervised by a teacher or adult.

- Pupils should be taught skills and techniques to enable efficient and effective use of the Internet.

- Pupils should have a clearly defined focus for using the Internet and e-mail.

- If offensive materials are found the monitor should be switched off, any printed materials or USBs should be confiscated and offensive URLs should be given to the IT Co-ordinator who will report it to the Internet Service Provider (ISP).

- Virus protection has been provided by the school as viruses can be down loaded accidentally from the Internet. Pupils bringing work from home, on memory stick / USB, could also infect the computer so this should be resticted.

- The ISP will check sites visited by schools.

- Pupils are not allowed to use open forums such as newsgroups or chat rooms.

- Disciplinary action may be taken if the Internet is used inappropriately e.g. for accessing pornographic, racist, extremist or offensive material, for personal financial gain, gambling, political purposes or advertising.

- Software should not be downloaded from the Internet (including screen savers, games, video clips, audio clips, *.exe files). Without the permission of the IT Co-ordinator or school technician

I have read the Code of Practice for pupils and Support Staff and I am familiar with the school's policy on the use of the Internet, e-mail, the creation of web sites and network security.

I agree to abide by these policies and the Code of Practice for Teachers

Name……………………………………………Signed…………..…………………………Date……….……

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If any member of staff violates these provisions, access to the Internet will be denied and they will be subject to disciplinary action.

Support Staff's Internet Code of Practice

- Support Staff should be familiar with the school's Network, Internet, e-mail and web site creation policies and the pupils' code of practice for Internet use.

- Support Staff should closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages.

- Computer monitor screens should be readily visible, so they can monitor what the pupils are accessing.

- Pupils should have clear guidelines for the content of e-mail messages, sending and receiving procedures.

- Use of the Internet should be supervised by an adult.

- Pupils should be taught skills and techniques to enable efficient and effective use of the Internet.

- Pupils should have a clearly defined focus for using the Internet and e-mail.

- If offensive materials are found the monitor should be switched off, any printed materials or USBs should be confiscated and offensive URLs should be given to the IT Co-ordinator who will report it to the Internet Service Provider (ISP).

- Virus protection has been provided by the school as viruses can be down loaded accidentally from the Internet. Pupils bringing work from home, on memory stick, could also infect the computer - some viruses will format your hard disc!

- The ISP will check sites visited by schools.

- Pupils are not allowed to use open forums such as newsgroups or chat rooms.

- Disciplinary action may be taken if the Internet is used inappropriately e.g. for accessing pornographic, racist, extremist or offensive material, for personal financial gain, gambling, political purposes or advertising.

- Software should not be downloaded from the Internet (including screen savers, games, video clips, audio clips, *.exe files). Without the permission of the IT Co-ordinator or school technician

I have read the Code of Practice for pupils and Support Staff and I am familiar with the school's policy on the use of the Internet, e-mail, the creation of web sites and network security.

I agree to abide by these policies and the Code of Practice for Support Staff.

Name……………………………………………Signed………….…………………………Date……………