The Kite Primary Federation

E-Safety Policy

Including acceptable use of:

1. The Internet;
2. Mobile Phones;
3. Cameras; and
4. Social Networking

Description:	This document outlines the Federation's policy on E Safety
Status:	Non Statutory Policy
Policy Audience:	Staff, Pupils & Parents/Carers
Federation Contact:	EHT, Finance Officer, H&S Governor
Other related Federation policies and procedures:	Health and Safety , Social Networking
Governor Committee:	Policies
Approved :	Autumn Term 2019
Frequency of review:	Annual
Latest Date for Next Review:	Autumn Term 2020

Teaching and Learning:

Use of the Internet:

The Federation recognises that 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.

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across 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 the LA and DfE;
- Access to learning, wherever and whenever convenient.

Using the Internet to Enhance Learning:

- The School Internet access will be designed expressly for educational use and the purposes of running the school and will include filtering appropriate to the age of pupils.
- Pupils will be 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. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff will guide pupils in online 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.

Evaluating Internet Content:

- The Federation will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be 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 a part of every subject.

Internet Access:

- The Federation , via its IT provider, will maintain a current record of all staff and pupils who are granted access to the Federation 's electronic communications.
- Internet access will be supervised, and children will be encouraged to use previously vetted websites used through favourites. Children will be taught how to use safely a variety of search engines and be taught specific skills in locating information effectively using search engines.
- Pupils will sign the Home School Agreement, which includes using the Internet responsibly. These are also signed by parents.
- We provide information and guidance via the school's website and the Federation 's newsletter for parents and children to cover internet safety and ways to protect children online.

Acceptable Use of Internet Statement:

The computer system is owned by the Federation and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and engagement. The Federation reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited and emails sent. Staff and KS2 pupils using Internet access should sign a copy of the "Expectations for Responsible Internet Use" and return it to the school office. An example is found at Appendix 1.

Managing Communication:

E-Mail:

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details about themselves or others in e-mail communication or arrange to meet anyone without specific permission.

- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on Federation headed paper.
- The forwarding of chain letters is not permitted.
- Pupils and staff should be aware that Federation e-mail might be monitored.
- All staff will have access to work e-mail addresses that will form an integral part of communication within the school.
- Access in school to external personal e-mail accounts are blocked. (e.g. Hotmail accounts)
- All e-mail (both incoming and outgoing) is checked for banned words and for viruses. Any breach of content is reported and dealt with.

Mobile phones and cameras:

- Staff in EYFS will use the school cameras to record observations of children's learning and development only. These cameras are purchased specifically for this purpose and when not in use, are kept in a secure cupboard. The cameras will always be accessible to the Designated Safeguarding person for inspection .
- Photographs are stored on the camera or school laptops only when being used for assessing or communicating learning and development. Photographs of the observations are printed regularly, and the memory card is then wiped clean.
- Where members of staff or parents are authorised to take photos on behalf of the school, they may use their own equipment, but school will provide the memory card/stick, which will be signed in or out of school.
- Mobile phones are to be used in line with the Staff Code of Conduct. Staff are not permitted to use mobile phones to photograph or record children or adults, but instead must use the school cameras purchased for the purpose.
- It is inappropriate for children or parents to contact members of staff on their mobile phone.
- Mobile phones will not be used during lessons or formal school time.
- Mobile phones should not be used in the corridors or in learning areas during the school day.
- The sending of abusive or inappropriate text messages is unacceptable.
- Children will not use mobile phones in school. If they bring a phone to school, because they need it when walking home, they must give it to their class teacher and collect it at the end of the day.
- Staff, parents and governors should not publish photographs of pupils other than their own children, in any media, including social networking sites and on Twitter, without the prior written permission of that child's parents or carers.

Published Content:

The School Website:

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.
- The Executive Head Teacher and governing board will take overall editorial responsibility and ensure that content is accurate and appropriate.

Pupils' Images or Work:

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Parents or carers are asked to return a signed form if they do not wish images of their children to be used electronically.

Managing Social Networking and Personal Publishing:

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind, which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph that could identify the student or his/her location e.g. house number, street name or school.
- Staff are advised not to run social network spaces for student use on a personal basis. Staff are advised to be cautious of information shared on social network sites and be mindful of who has access to this information and the importance of good security settings.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and are instructed on how to block unwanted communications. Pupils 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 social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Pupils will be shown how to publish and present information to a wider audience.

Managing Filtering:

- The school will work with the LA, and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the Executive Head Teacher.
- The school's filtering is managed by West Berkshire, and any portable devices will be set up with appropriate age filters.
- Any material that the school believes is illegal must be reported to the Executive Head Teacher who will report it to appropriate agencies such as IWF or CEOP.

Managing Information Systems:

Security & Protecting Personal Data:

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Risk Assessment:

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use. Websites to be used during a lesson or recommended for Home Learning should be checked prior to use for inappropriate content, e.g. advertisements, although it is acknowledged that these can change between this check and the site being used by pupils.

- The school audits ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Handling E Safety Complaints:

- The Executive Head Teacher or a school governor will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Head Teacher
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Implementing this policy:

With children:

- All children are made aware of E-Safety rules.
- Pupils are informed that network and Internet use will be monitored.
- The school incorporates e-safety learning into ICT learning to raise the awareness and importance of safe and responsible Internet use.
- Instruction in responsible and safe use of the Internet is an integral part of ICT learning in school.

With staff:

- All staff have access to the School E-Safety Policy and its application and importance explained.
- Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.

With Parents / Carers:

- Parents' attention will be drawn to the school's E-Safety Policy through the school prospectus, on the school website and through the training offered on an annual basis.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents is encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use.

Signed…………………………………………………….Chair of the Governing Board

Signed……………………………………………. Executive Head Teacher

Date…………………………………………………

Appendix 1

Expectations for Responsible Internet Use

The Internet enhances your learning opportunities and offers you a wealth of information, but you need to be responsible for your own use of the Internet. The following rules will ensure your surfing of the Internet is safe and successful.

- I will only use the Internet when I have been given permission from a member of staff.
- I will ensure there is an adult supervising when I use the Internet.
- I will use the Internet appropriately for e-mails, home learning or learning for school.
- I will only e-mail people I know, or whom my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given me permission.
- I will report any unpleasant material or messages sent to me to a Teaching Assistant or Teacher. I understand my report would be confidential and would help to protect other pupils and myself.

- I understand that the school may check my computer files and may monitor the Internet sites that I visit.
- I will only access my own e-mail account with my password, which I will keep secret.
- I will not access other people's files or use their login unless given permission by an adult.
- I will not plagiarise by using work off the Internet as my own.
- I will not bring in pen drives or discs from outside school unless I have been given permission. This is to help stop computer viruses from spreading.

Signed……………………………………………………………Pupil

Date…………………………………………………………….