E- SAFETY POLICY

Approved by Staffing & Curriculum Committee: January 2014
Review Date: January 2017

Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

1. Why is Internet use important?

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

2. How will Internet use enhance learning?

The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils. Staff should 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.

3. How will Internet access be authorised?

Primary pupils' home-school agreement will include the acceptable use policy and guidance for video, sound and images for web publication. Primary pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision. At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials. Parents will be informed that pupils will be provided with supervised Internet access.

4. How will filtering be managed?

A designated member of staff will manage the permitting and banning of additional web sites identified by the school. The school will work in partnership with parents; Wiltshire County Council, DCFS and the Oakford to ensure systems to protect pupils are reviewed and improved.

Staff will ensure that regular 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 referred to the Internet Watch Foundation (IWF - http://www.iwf.org.uk/).

5. Managing content

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to Oakford Web Filtering

Specific lessons will be included within the curriculum that teaches all pupils how to develop their media literacy skills, in particular validity and bias. At Key Stage 2, pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. Training should be available to staff in the evaluation of web materials and methods of developing students' critical attitudes.

6. How should website content be managed?

The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Website photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the pupils to be identified. The Staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

7. Managing e-mail

Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive emails. Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone. Whole-class or group e-mail addresses should be used at Key Stage 1 & Key Stage 2. Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly. Access in school to external personal email accounts is not allowed. E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

8. On-line communications and social networking.

The school will conduct regular pupil surveys (three-yearly or ideally more often) about home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc. The use of online chat is not permitted in school, other than as part of its online learning environment.

9. Mobile technologies

Mobile phones are not permitted within the school. Pupils/students will be asked to give them to their teacher/tutor at the start of the school day.

10. Introducing the Policy to Pupils

Rules for Internet access will be posted in all rooms where computers are used. Instruction on responsible and safe use should precede Internet access. Pupils will be informed that Internet use will be monitored. The teaching of e-safety will be part of the curriculum for all pupils throughout the year.

11. Parents and E-Safety

Parents' attention will be drawn to the school e-Safety policy in newsletters, and on the school Website. Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home. There will be a parents evening at least once a year about E-safety which will include suggestions for safe Internet use at home. Interested parents will be referred to organisations such as Childnet International, PIN, Parents Online and NCH Action for Children.

12. Consulting with staff and their inclusion in the e-safety policy

All staff including teachers, supply staff, classroom assistants and support staff, will be asked to sign the Policy for responsible e-mail, network and Internet use. The school's consequences for Internet and mobile phone/PDA/technology misuse will be clear so that all teachers are confident to apply this should the situation arise. Staff should be aware that Internet traffic is monitored and reported by the Oakford and can be traced to the individual user. Discretion and professional conduct is essential. The monitoring of Internet use is a sensitive matter.

13. How will complaints be handled?

Responsibility for handling incidents will be delegated to the Headteacher. Parents and pupils will need to work in partnership with staff to resolve issues. There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Kennet Valley School

Responsible Internet Use

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

- I will ask permission before using the Internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. Oakford monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.

Glossary of Terms

Blog – Short for Web Log, an online diary

DCSF - Department for Children, Schools and Families

Podcast – a downloadable sound-recording that can be played on computers and MP3 players

Oakford – which provides Internet access and associated managed services to all schools in the South West

Social Networking – websites that allow people to have "pages" that allow them to share pictures, video and sound and information about themselves with online friends

Video Blogging – online videos that can be uploaded via a web cam

Web 2 Technologies – a collection of online web services that are based around communicating/sharing information