KINETON GREEN PRIMARY SCHOOL

INTERNET ACCEPTABLE USE POLICY 2019

T.Coldrick
June 2019

Introduction

The acceptable use policy links to the schools Computing policy. It has been written by the Computing subject leader using information from the Superhighway Safety website and guidance from Solihull Primary ICT team.

Why is Internet use important?

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 information and business administration systems.

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

How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives such as the DfES ICT in Schools and the Virtual Teacher Centre (VTC) **http://vtc.ngfl.gov.uk**;
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LEA and DfES.
- Mentoring of pupils and provide peer support for them and teachers

How will Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable, what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities, across all subject areas. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line 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

How will pupils learn to evaluate Internet content?

- Pupils will be taught specific, year group appropriate, e-safety lessons prior to accessing the internet, based on the e-safety modules in the Solihull Primary Computing Scheme of Work.
- In KS1 children will only use www.kidsrex.org to complete online searches as it is a safer, more child friendly version of www.google.co.uk.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the computing co-ordinator.
- Schools should 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 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.
- Training should be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts on the school system.
- Each pupil will have an individual password for their email that they will not share with any other person. They will be taught about the danger and implications of sharing passwords.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address, telephone number, or age or arrange to meet anyone.
- Access in school to external personal e-mail accounts may be blocked.
- 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.
- The forwarding of chain letters is not permitted.

How should Web site and Twitter page content be managed?

- The point of contact on the Web site and Twitter page should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site and Twitter photographs 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 Web site or Twitter, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or Twitter.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Newsgroups and Internet chat

- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.
- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.
- Use of Facebook and other social sites will not be permitted in school. The school's Twitter is only for access by staff, all of whom have been given a copy of the Twitter Use Protocol, detailing simple do's and don'ts for its use. Staff may use Facebook for social purposes outside of school, but must set their profile so they are 'private' and personally identifiable information and updates are not publicly visible.
- The PTA have a Facebook Page set up by the Local Authority and this is a 'closed group'. Only approved members can be invited and the Head Teacher is able to view content on this page.

Intranet

- Pupils will be taught about the differences between internet and intranet and the educational benefit of using both.
- Use of the intranet, WIKIs, discussion groups and blogs will be fully supervised in class.
- Pupils will accept that the messages they may post will be polite and sensible.
- Parents permission will be obtained prior to children being able to access the Intranet from home.
- Teachers will review and accept children's blogs prior to them being posted on the Intranet, within guidelines given by Solihull MBC.

Web conferencing

- Pupils will be taught how to safely use webcams for the purpose of educational benefit.
- All external web conferences will be check by the teacher prior to children being able to access them.
- All web conferencing will be in the presence of a member of staff.

How can emerging Internet applications be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

How will Internet access be authorised?

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Websites will be saved onto the shared drive for children to access, rather than the children using a search engine to find it.
- Parents will be informed that pupils will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form

How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

How will filtering be managed?

- The school will work in partnership with parents, the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. Filtering is managed by Solihull MBC.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to council team via the ICT co-ordinator.

How will the policy be introduced to pupils?

- Rules for Internet access will be posted in all rooms where computers are used.
- Simple E-Safety posters are up in all classrooms.
- Pupils will be informed that Internet use and any messages posted on the Intranet will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- E safety lessons will be planned in and delivered for each year group and monitored.

How will staff be consulted?

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.
- Staff training will be provided when required to ensure all staff are up to date on current Computing guidance.

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LEA, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
- All teaching staffs' laptops and memory sticks are fully encrypted.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - informing parents or carers;
  - removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).
- Parents of new pupils joining will be provided with a copy of the School Internet policy and a CD Rom of how to keep safe online.

Kineton Green Primary 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 own network login and password, which is secret.**
- **I will only look at or delete my own files.**
- **I understand that I must not bring software or disks into school without permission.**
- **I will only e-mail 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.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **I will not use Internet chat.**
- **If I see anything I am unhappy with or if I receive messages I do not like, I will tell a teacher immediately.**
- **I understand that the school may check my computer files 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.