The E-Safety Policy

1. Who will write and review the policy?

- Our E-Safety Policy has been written by the school, building on the KCC policy and government guidance. It has been agreed by the staff and approved by governors. It will be reviewed on an annual review cycle.

Revised by: Mrs Rose Cope (E-safety Officer)
Governor: Mrs Chantal Wayman

Date: November 2015

Next revision: November 2016

Approved:

Teaching and Learning

2. 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 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 children with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Internet access is an entitlement for students

3. The benefits of the Internet on education

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- 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 networks of schools, support services and professional associations;
- Educational and cultural exchanges between pupils world-wide.
- Staff professional development through access to national developments, Educational materials and good curriculum practice.

- Communication with support services, professional associations and colleagues.
- Exchange of curriculum and administration data with the LEA and DfES.
- Extending the potential for home learning through Learning Platforms.
- Communication to parents through the use of parent mail thereby protecting the environment.

4. Internet use enhances 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 is acceptable and what is not acceptable 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 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 and retrieval.
- Pupils will receive regular child led sessions on e safety and the use of social networking websites outside of school.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

5. Pupils will be taught how to evaluate internet content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the E-Safety Officer (Rose Cope).
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Training should be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

6. Maintaining information systems security

Local Area Network security issues include:

- Users must act reasonably- e.g. the downloading of large files during the working day will affect the service that others receive.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- The virus protection for the whole network must be installed and current, this must include staff laptops.

Wide Area Network (WAN) security issues include:

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discuss with EIS.
- Portable media may not be used without specific permission followed by a virus check, e.g. floppy disks, CDs and memory sticks. Memory sticks used by staff should be provided by the school.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

7. Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail (Inappropriate content includes offensive language, homophobic, xenophobic, racist and personal attacks).
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Children will use their VLE email accounts to communicate with other members of the VLE only, unless approved and released by the VLE Manager.
- Whole-class or group e-mail addresses should be used at Key Stage 2 and below where emails extend outside the school community.
- Some approved VLE domain addresses can be released by the VLE manager with regard to penpal work.
- 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. Managing published content

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' personal information must not be published.
- The Head teacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.

- The copyrights of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

9. Publishing images of children and children's work

- Web site photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs
- Written permission from parents or carers will be obtained before photographs of pupils and pupil's work are published on the school Web site or local newspapers.(See appendices 1 & 2).
- Images used on the VLE (DB Primary) do not need parental permission as this is within the school environment and inaccessible outside of the VLE.

10. Social networking and personal publishing

- Pupils will be not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will always be supervised and the importance of chat room safety emphasised.
- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.
- Children will be informed of safe use of newsgroups and chat rooms outside of school and parents supported in understanding how to monitor their children's internet use at home.
- E-safety scheme of work includes sections on cyber bullying of all forms including homophobic, xenophobic and racist.
- 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, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

11. Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and web cam use will be appropriately supervised for the pupils' age.

11. Managing filtering

- The school will work in partnership with parents; the KCC, Becta and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.
- Senior 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 (please see references given later).
- Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

12. Emerging technologies

- 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. They should be given to office staff to look after at the beginning of the school day and collected from the office at the end of the day. The sending of abusive or inappropriate text messages is forbidden. If incidents of this are discovered parents will be invited in to discuss.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications
- Games machines including the Sony Playstation, Nintendo DSi, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Policy Decisions

13. 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 leaving or the withdrawal of a pupil's access.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource. (See appendix 3)
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is included as an appendix).
- Parents will be asked to sign and return a consent form. Please see the sample form later in this document.

14. Assessing the risks

- 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. Neither the school nor KCC can accept liability for the material accessed, or any consequences of Internet access.
- 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 Head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

15. Handling complaints regarding e-safety

- Responsibility for handling incidents will be delegated to the E-safety Officer (Mrs Rose Cope DCPC).
- Any complaint about staff misuse must be referred to the Head teacher.
- 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:
    - -discussion with the E-Safety Officer or Head teacher;
    - -informing parents or carers;
    - -removal of Internet or computer access for a period.

Communications Policy

16. Introducing the policy to pupils

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access and regular assembly time provided to review safe use in school and at home.
- The teaching and learning about responsible Internet use will be embedded throughout the curriculum, covering both school and home use.
- An E-Safety training programme will be embedded into the curriculum and key stage assembly content to raise awareness and importance of safe and responsible Internet and mobile phone use.

17. Informing staff

- All staff including teachers, classroom assistants and support staff, will be provided with the School E-Safety Policy, and its importance explained. The –safety policy is also available to view on the school website
- 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 the safe and responsible Internet use, and on school Internet policy will be provided as required.
- Supply staff should be asked to prepare fully before taking charge of an Internet activity.

18. Enlisting parental support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the VLE.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This will include parent workshops with demonstrations and suggestions for safe home Internet use. Regular pamphlets on safety will be sent out and websites of use will be on the school newsletter as they are discovered.

Appendices

1. Letter that informs parents.
2. Consent form for parents to sign.
3. Staff Information Systems Code of Conduct.
4. Staff guidance on teaching-E-Safety to young children.
5. E-Safety guidance for pupils with AEN.
6. Legal framework from 'Schools E-Safety Policy 2007'
7. List of useful websites on E-Safety.