EDWARD THE ELDER PRIMARY SCHOOL

E-SAFETY POLICY

Agreed with SMT and Approved by Governors:- June 2015

To be reviewed:- June 2016

Our Internet Safety Policy has been written by the senior management and approved by governors. It will be reviewed annually.

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 & for preparation for their future lives.

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
- 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 LA and DfEE.

How will Internet use enhance learning?

The school Internet access will be designed 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.

How will pupils learn to evaluate Internet content?

If pupils encounter material they feel is distasteful, uncomfortable or threatening, they should report the address of the site to a member of staff.

The use of Internet derived materials by staff and by pupils should comply 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 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.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Individual email addresses may be allocated for the use of pupils
- Access in school to external personal e-mail accounts will 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 banned.

How should Web site content be managed?

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- 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 will be sought before photographs of pupils are published on the school Web site.
- The head teacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate.
- 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 E Mail Lists

- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.

Chat Rooms.

- Pupils will **<u>not</u>** 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/application in school.

How can emerging Internet uses 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. (See use of mobile phones policy for more detail).

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.

- At Foundation Stage & Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Key Stage 2 pupils are taught to access & search the internet in a responsible manner. This will be supervised directly or remotely.
- Parents & pupils will be asked to sign and return a consent form. (see appendix 1). [Staff AUP Appendix 2]

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. We 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 Wolverhampton City Council 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.

How will filtering be managed?

The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task as new sites appear every day. School use the same filtering system purchased by Wolverhampton City Council.
- Dynamic filtering examines the content of Web pages or e-mail for unsuitable words. Filtering of outgoing information such as Web searches is also required.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content. This will be filtered by a combination of the Internet Service Provider, the LA, and at school-level.

Careful monitoring and management of all filtering systems will be required. It is important that the school establishes the filtering criteria rather than simply accepting filtering default settings.

- The school will work in partnership with parents; the LA, DfEE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate and effective.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Senior Management Team.

What should we focus on?

- Check the e-mail, chat and Web site.
- Discuss with pupils the Rules for Responsible Internet Use, primary version.
- Preview all sites before use and consider off-line viewing.
- Plan the curriculum context for Internet use to match pupils' ability.
- Vigilance is essential, supervision the most important strategy.

How will the policy be introduced to pupils?

- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible Internet use will be taught covering both school and home use.

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 the safe and responsible internet use and on school Internet policy will be provided as required.

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 LA, particularly where a wide area network connection is being used.
- Use of USB sticks will be reviewed. Personal USB sticks may not be brought into school without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The IT co-ordinator will ensure that the system has the capacity to take increased traffic caused by Internet use.
- Backup procedures are in place where all essential office data is backed up off site.

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 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 for pupils include: - interview/counselling by head teacher; - informing parents or carers; - removal of Internet or computer access for a period, which could prevent access to school work held on the system. (See Appendix 3)

How will parents' support be enlisted?

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school prospectus 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.

Appendix 3

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.