Bentley Heath C of E Primary School
E-Safety Policy

Our e-Safety Policy builds on the SMBC Schools' e-Safety Policy and government guidance. The e-Safety Policy and its implementation will be reviewed annually; Governors, Parents and Staff will be consulted.

Roles and Responsibilities
Governors delegate to Headteacher/Assistant Headteacher. The School e-Safety Co-ordinator is Mr S Hawke, Assistant Headteacher and a designated member of staff responsible for Child Protection.

Mrs R Boam, ICT Leader, are responsible for operational/technical planning, implementation and oversight. All classroom-based staff are responsible for teaching safe and responsible usage in their subject areas.

The School recognises why Internet use is 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 functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- 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.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Safe Internet use to 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 and what is not and will be given clear objectives for safe 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, retrieval and evaluation.

Safe and Responsible Use – Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

- An e-Safety training programme is delivered to all pupils during their KS2 ICT lessons to raise awareness and the importance of safe and responsible use of the Internet and other electronic communications tools.

Safe and Responsible Use – Staff

- All staff will be given the School e-Safety 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.
- Staff that manage filtering systems (currently the ICT technical team) or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required. Policy consultation, regular reminders via Bulletin/Briefings, individual advice from Assistant Headteacher/Headteacher.

Safe and Responsible Use – Parents

- Parents attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school website.
- Internet issues will be handled sensitively to inform parents without alarm.
- A partnership approach with parents will be encouraged. This could include parents' evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents on request.

Internet Access

- All users must read, sign and abide by the "Acceptable ICT Use Policy" before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by directly supervised access to specific, approved on-line materials.
- KS2 pupils must agree to comply with the Responsible Internet Use statement before they are granted access.
- Parents will be asked to sign and return a consent form for pupil access.
- The school recognises that 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 e-Safety Policy is implemented and compliance with the policy monitored.

Pupils Evaluating Internet Content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Solihull ICT Services, and where appropriate the school e-Safety Officer.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- They 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 using the Internet.

Managing the School's Public Website

- The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- E-mail addresses should be published carefully to avoid spam issues.
- The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- The Network Manager is responsible for ensuring that the overall content is accurate and appropriate.

Publishing Images of Pupils

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- If a name is to be used with a photograph which identifies a student, for example in a press release, we will ask permission from parents.

Managing Social Networking

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils will be 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 will be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name, school or shopping centre.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should not run social network spaces for students on a personal basis. Teachers should not communicate with pupils through private social networking sites, even on educational matters, but should use official sites sponsored by the school.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others. They should be 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 set up without a password and others are invited to see the bully's comments. Incidents of bullying through social networking will be dealt with in line with the school policy on bullying.

Managing Filtering

- The school will work in partnership with Solihull MBC to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school e-Safety Co-ordinator.
- We are aware of the need to ensure that filtering policies take account of new developments on the Internet.

- The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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 e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Use of words included in the filtering/checking "banned" list will be detected and logged.
- E-mail should be supervised in a manner appropriate to the age of pupils concerned.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations 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.
- E-mail addresses should be published carefully to avoid spam harvesting.

Video Conferencing

(We do not currently have video conferencing facilities but include draft statements in the Policy to take account of statutory requirements).

- The equipment and network
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites. Video conferencing contact information should not be put on the school website.
- School video conferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.
- The equipment must be secure and if necessary locked away when not in use.
- Users
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Video conferencing should be supervised appropriately for the pupils' age.
- Responsibility for the use of the video conferencing equipment outside school time needs to be established with care.
- Only key administrators should be given access to the video conferencing system web or other remote control page available on larger systems.
- Unique log on and password details for the educational video conferencing services should only be issued to members of staff and kept secure.
- Content
- Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).
- Video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

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. The sending of abusive or inappropriate text messages is forbidden.
- Risk Awareness: The School recognises the pace of change in communication and the necessity for on-going assessment of new and emerging risks.
- Staff will be issued with a school phone where contact with pupils is required.

Managing Information Services

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will follow Solihull MBC guidelines.
- 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. Where they are used to store personal information they will be encrypted.
- 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 Network Manager will review system capacity regularly.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available in compliance with the Data Protection Act 1998.

E-Safety Complaints

- Formal complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher who should use the agreed procedures.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions for pupils within the school discipline policy include:
- Interview/counselling by Lead Tutor or senior leader
- Informing parents or carers
- Removal of Internet or computer access for a period
- More serious sanctions/exclusion if bullying or repeated misuse.

Community Use of ICT and the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.