Bramley Sunnyside Infant School

E-Safety Policy

Date of initial approval:	**January 2015**
Amended:	**First issue**
Review date:	**January 2016**

Revision History		
Version	Reason for issue	Approval date
1.0	Revised publication for approval by Governing Body	January 2015
1.0		

Bramley Sunnyside Infant School
E-Safety Policy

Our e-Safety Policy forms part of the Acceptable Use Guidance, building upon government legislation, to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

It has been agreed by the senior leadership team, staff and children and approved by governors.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for our children but everyone within our school community lies in the effective education that we provide. We know that the Internet and other technologies are embedded in children's lives not just in school but outside as well and we have a duty to help prepare our children to safely benefit from the opportunities the Internet brings.

- The Internet is an essential element in 21st century life for education. In addition, the school has a duty to provide children with quality Internet access as part of their lifelong learning.

- The purpose of Internet use in school is to raise educational standards, to promote children's achievement, to support the professional work of staff and to enhance the school's management information systems.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and children. Internet access is an entitlement for students who show a responsible and mature approach to its use.

- Curriculum activities that involve the use of the Internet for gathering information and resources will develop children's skills in locating and evaluating materials.

- Children will be taught how to validate materials they read before accepting their accuracy.
- Other techniques for research will be developed through the use of a limited group of school approved sites.
- Where materials gathered from the Internet are used by children in their own work, they will be taught to acknowledge the source of information used.
- The school will ensure that the use of Internet materials by staff and children complies with copyright law.

Acceptable Use

- As part of the curriculum, our children are made aware of the guidelines for the acceptable use of the Internet and what is not acceptable usage. This is enhanced through our SEAL, PSHCE lessons, and visits by Year 6 to Crucial Crew and through visitors to school.
- Guidelines for acceptable use are clearly on display in all areas of the school where Internet access is available.

- All children are given clear objectives when using the Internet.
- Where Internet activities are part of the curriculum they are planned so that they enrich and extend the learning activities.
- Staff guide children through on-line activities that support the learning outcomes planned for the age and maturity of the children. Example, websites are often provided for the children as hyperlinks within their task instructions, in this way ensuring links that the children access are relevant and appropriate to their work.
- All websites used for specific activities will have been approved by the school.
- Training is available to staff in the evaluation of Internet materials.

Managing ICT Systems and Access

Information System Security

- School ICT systems security are reviewed regularly.

- Virus protection is also updated regularly.

- Security strategies are in line with Local Authority guidance.

E-Mail

- Curriculum activities that involve the use of e-mail are through the use of class or group webmail accounts that are controlled by the school.
- All e-mail communications sent by members of staff that relate to the school will be through authorised, school controlled webmail accounts.
- The use of individual pupil personal accounts is not permitted through the school system.
- Any e-mail sent to an external account is authorised by the school, before sending, following the same procedure used for letters written on school headed notepaper.
- Children will never reveal personal details of any member of the school community in e-mail communications.

Published Content and School Website

- The school website is maintained and kept up to date.
- The headteacher ensures that the content is accurate and appropriate to the needs of the school community.
- No personal information about any member of the school community will be published on the website. Written permission from parents or carers is obtained before photographs of children or names are published on the website.
- Only first names of children will be published.

Managing Filtering

- Internet access in the school is provided via a broadband link through RGFL.

- Filtering appropriate to the age of the children is provided as part of this link.

- An agreement for the provision of a suitable virus protection system has been implemented through RGFL.

- This virus protection system will be installed on all computers in school and automatically updated regularly.

- The school Internet access has been designed especially for pupil use and includes filtering appropriate to the age of the children.

Managing Emerging Technologies

- This e-safety policy considers the use of both the fixed and mobile internet, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, personal digital assistants and portable media players.

- It will be revised to incorporate new and emerging technologies.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- The school will ensure that all members of the school community are aware of the e-safety policy and the implications for the individual.

- E-safety depends on staff, governors, parents and, where appropriate, the children themselves taking responsibility for the use of Internet and other communication technologies.

- Portable media may not be brought into school without specific permission and a virus check.

- Children's access to the Internet will be by adult demonstration or directly supervised access to specific, approved on-line materials.

- Responsible and safe use when using the Internet is always discussed with children before access is permitted.

Protecting Personal Data

- Personal data will be recorded, processed and transferred and made available according to the Data Protection Act 1998.

Assessing Risks

- The headteacher will ensure that the e-safety policy is implemented and compliance with the policy monitored.
- Some material available on the Internet is unsuitable for children therefore will not be used in school.
- Methods to identify, assess and minimise risks are reviewed regularly. For example, staff will always thoroughly check website content before it is accessed by children. All e-mails received and sent will be read by class teachers.
- Whilst school takes all reasonable precautions to ensure that children access only appropriate material, due to the nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

- It is important to state that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Handling E-Safety Complaints

- Where unsuitable content is encountered staff and children should follow the school procedures for such events.
- Unsuitable URL addresses will be reported through the school office to the LA technical support team.
- Children must report unsuitable material, including e-mail content, immediately to a teacher.
- The teacher will then ensure that the reporting procedures are followed.
- Parents will be informed of such incidents sensitively to avoid undue distress.
- Where incidents occur due to non-compliance with the school e-safety policy these will be reported to a delegated senior member of staff.
- Any issues relating to staff misuse must be referred to the headteacher.
- Should it become necessary to prohibit the use of internet resources for a child then parents or carers will be involved so that a partnership approach can be used to resolve any issues.
- This could include practical sessions and suggestions for safe Internet use at home.

Staff and the E-Safety Policy

- All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school e-safety policy.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user and professional conduct is essential.
- Staff development in safe and responsible Internet use will be provided as part of the continuing professional development programme.
- The school will keep an up-to-date record of all staff and children who are granted Internet access.
- Staff will be fully aware and adhere to the social networking policy. (October 2012)

Enlisting Parents' and Carers Support

- A consent form, which covers permission to access the Internet, will be issued to parents and carers during the summer term to cover the forthcoming academic year. This will contain the acceptable use guidelines and details of the school e-safety policy.
- Parents and carers will be required to sign the consent form and where appropriate children will also be required to sign an acceptance of both the acceptable use guidelines and the e-safety policy.
- The signed consent form must be returned to the school for children's access to the Internet to be permitted. Children will be informed that Internet use will be monitored.
- Children's access may be withdrawn if the acceptable use guidelines are not adhered to.