Bowling Park Primary E-safety Policy is based on:

- **Our Vision for ICT**
- **Our School Improvement Plan**
- **Guidance from Bradford Council and other partners**
- **The Data Protection Act (1998)**

Priorities for developing and implementing the E-safety Policy:

- **Developing our vision for ICT**
- **Developing our e-safety curriculum for all students**
- **Training and guidance notes for all school staff**
- **Guidance notes for all parents / carers (translated as appropriate)**
- **Developing Policy on use of images of children and staff**
- **Developing staff code of conduct on the use of ICT**

Our Vision for ICT

Information and Communication Technology (ICT) contributes to the school curriculum by preparing all young people to participate in a rapidly changing society in which work and other forms of activity are increasingly dependent on ICT. The subject develops pupils; "information skills, including the ability to use information sources and ICT tools to help them find, explore, develop, analyse, exchange and present information and to support their problem solving, investigative and expressive work." An essential part of ICT capability is being discriminating about information and the ways, in which it may be used, and making informed judgments about when and how to apply aspects of ICT to achieve maximum benefit. Pupils also develop understanding of the implications of ICT for working life and society. The use of ICT significantly enhances teaching and learning in other subjects by enabling rapid access to knowledge, information and experiences from a wide range of sources. The use of ICT throughout the curriculum encourages critical thinking, imagination and creativity, problem solving, initiative and independence, teamwork and reflection.

"We interpret the term 'information communication technology' to include the use of any equipment which allows users to communicate or manipulate information (in the broadest sense of the word) electronically."

Our E-safety Policy

The school has a named e-Safety Officer. This is the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.

Bowling Primary e-Safety Policy has been written by the school, building on advice from Bradford Council, Datacable and relevant national guidance.

RATIONALE

1. Teaching and learning

Why the Internet and digital communications are important.

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- All pupils and will have access to ongoing e-Safety advice and training.

2. Access to the Internet to enhance learning

- The school Internet access will be designed expressly for pupil use and we have introduced filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. All classes negotiate and agree their own e-safety guidelines.
- Pupil access to the Internet will only be permitted under the supervision of an appropriate adult.
- Pupil access to the Internet via Windows based devices will be monitored using Forensic Monitoring Software. We are currently investigating safe browsers for Apple devices.
- Access to the Internet will be planned to enrich and extend learning activities.
- Access to the Internet will be regularly reviewed to match the curriculum requirements and age of pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will receive regular e-safety learning, including: blogging safely, navigating the internet and social networks, evaluating content and safe publishing. E-safety is one of the themes of our SMSC assemblies.

3. How will pupils learn how to evaluate Internet content?

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be shown how to publish and present information to a wider audience as the technologies develop (i.e. using the school blog, bowlingparkprimary.net).
- Pupils will be taught how to recognise and report inappropriate content. Inappropriate content is to be reported to an appropriate adult and then to the e-safety team. An e-safety report button is accessible on all devices and blog pages.
- Filtering and protection systems will be regularly reviewed and updated by the e-Safety Officer, the ICT team and relevant partners.

4. Managing information systems security

- The security of the school information systems will be reviewed regularly by Datacable, Bradford Council and the e-safety team.
- Curriculum data will be backed up regularly by Datacable and stored securely. Admin data will be backed up by Bradford Council and stored securely.
- Virus protection will be updated regularly by Datacable.
- The ICT team will regularly review system capacity.

5. Published content and the school website

- Staff or pupil personal contact information will not be published.
- The contact details given online will be the school address, telephone and email.
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with school's guidelines for the publications, including respect for intellectual property rights and copyright.
- The content of the website will be regularly reviewed and updated according to current government and Ofsted guidance.

6. Publishing pupils' images and work

- Pupils' full names will not be used anywhere on a school website or other on-line space.
- Parents are given the opportunity to opt out of their child's image being published
- A register of children without consent will be kept by the e-Safety Officer and their images will not be published in accordance with the parent's wishes.
- Images and video must be captured using school devices only. With prior arrangement with the Principal, an individual member of staff may use their own equipment in line with the Data Protection Act 1998. All images of children must be stored securely on the school network.

7. Social networking and personal publishing

- The school will control access to social networking sites, and educate pupils in their safe use.
- Access to social networking sites will be limited to Upper KS2.
- Pupils will not be allowed to access conventional social networking sites (Facebook, MySpace, Ask.fm, Bebo etc).
- The school will filter and limit access to social networking sites in languages other than English.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Pupils will be advised to use nicknames and avatars when using social networking sites.

8. Managing filtering

The school will work with Bradford Council and Datacable to ensure systems to protect pupils are consistently reviewed and updated.

- If staff or pupils come across unsuitable online materials, the site must be reported to the e-Safety Coordinator and the ICT team. The ICT team is able to block inappropriate websites using Smoothwall web filtering.
- A 'report an e-safety concern' button is present on the school blog, and can be completed by any child or adult. This form is sent directly to the senior leadership team.
- The ICT team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The e-Safety Coordinator will monitor staff and pupil access to the Internet using Policy Central Forensic Software.
- Staff will monitor comments on the school's blog and report any concerns to the e-Safety co-ordinator.
- Violations will be reported to the e-safety officer in the first instance and subsequently to the ICT team and Principal.

9. Managing new technologies

Mobile Phones

- The leadership team notes 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.
- Mobile phones will not be used by staff or pupils during lessons, except by prior arrangement with the Principal.
- The sending of abusive or inappropriate text messages or files by Bluetooth, WiFi or any other means is forbidden.
- Pupils are not allowed to use personal mobile phones or devices in school time, except by arrangement. Pupils are required to hand their mobile phones and personal devices into the school office at the start of the day. This Policy will be reviewed regularly.
- Personal mobile phones will not be used to capture images of children.
- Violations will be reported to the e-Safety Officer in the first instance and subsequently to the ICT team and Principal.

10. Copyright

- All software loaded on school computer systems must have been agreed with the ICT Team.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Images and resources published electronically out of school, on blogs, websites, social networking sites must be obtained from copy-free sites or comply with the terms of the license under which the materials were issued.

11. Data Protection Act 1988

The school is registered with the relevant Data Protection authority. It will ensure that it adheres to the Data Protection Act of 1998. It will ensure that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subjects rights
- secure
- not transferred to other countries without adequate protection

- Identifying data covered by the Data Protection Act 1998 (Type Two data) cannot be taken out of school except on an encrypted memory stick. This will be discouraged unless absolutely necessary

12. Authorising internet access

- Internet access is an essential part of the statutory curriculum.
- All staff must read and sign the Bowling Primary Acceptable Use Policy for ICT before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Any person not directly employed by the school will be asked to sign an Acceptable Use Policy before being allowed to access the school network and internet.

13. Assessing risk

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Bradford Council can accept liability for any material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-safety Policy is appropriate and effective.
- The e-safety Policy will be reviewed termly by the e-Safety team.

14. Handling e-Safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff and referred to the e-Safety Officer and ICT team.
- Any complaint about staff misuse of school ICT equipment or inappropriate use of social networking sites must be referred to the Principal. Complaints will be dealt with in line with the Disciplinary Procedure for School Staff.
- Complaints relating to child protection must be dealt with in accordance with school child protection procedures and e-safety policy.
- Pupils and parents will be informed of consequences for pupils misusing the internet.
- Discussions will be held with Bradford Council and other relevant parties to establish procedures for handling potentially illegal issues.

15. Introducing the policy to staff

- E-safety is an element of induction training for all new staff.
- Additional staff training in safe and responsible internet use and on the school e-Safety Policy will be provided at least annually.
- All staff are given the School e-Safety Policy and its application and importance explained.
- All staff, including visitors, sign the AUP policy.
- Staff are aware computer use is monitored and traced to the individual user.
- Staff responsible of managing filtering systems or monitoring ICT use will be supervised by senior management and have clear procedures for reporting issues.

16. Introducing the policy to children and families

- E-Safety rules are posted in all classrooms.
- Pupils are informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- E-safety will be a theme in SMSC assemblies, SMILE week and the wider curriculum.
- E-safety information is regularly provided to parents and the wider community through the weekly newsletter, the school blog and parents events.

The e-Safety policy has been written by a team with a wide range of experience and will be reviewed on a termly basis.

It has been agreed by the leadership team and approved by Governors.

Reviewed: September 2016