St Alban's Primary School

E-Safety Policy

Date	Review Date	School Lead	Nominated Governor
November 2018	November 2019	Martin Smith	Claire George

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
The previous Internet Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.
The school's e-safety policy will operate in conjunction with other policies including those for Positive Behaviour, Anti-Bullying, Curriculum, Data Protection and Security.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Newcastle LA Network including the effective management of Websense filtering.
- National Education Network standards and specifications.

E-Safety Audit

This quick self-audit will help the management team assess whether the e-safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an e-Safety Policy that complies with LA guidance?	Y
The Policy is available for staff at: school website and internal drives	
And for parents at: School website	
The Designated Child Protection Coordinator is: Mr Smith & Mrs Duncan	
The e-Safety Coordinator is: Mr Smith	
Has e-safety training been provided for both pupils and staff?	Y/
Do all staff sign an ICT Code of Conduct on appointment?	Y/
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules? (Older children agree to the rules)	Y/

Have school e-Safety Rules been set for pupils?	Y/
Are these rules displayed in all rooms with computers?	Y/
Internet access is provided by an approved educational Internet service provider and complies with DCFS requirements for safe and secure access.	Y/
Has an ICT security audit been initiated by the management team, possibly using external expertise?	Y/
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

School e-safety policy

2.1 Writing and reviewing the e-safety policy

The e-Safety Policy relates to the school's safeguarding policies and practices as well as to other policies including those for ICT, Anti-Bullying and Child Protection.

- The school will appoint an e-Safety Coordinator. This will be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by all staff and approved by Governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: Feb 2015
- It was approved by the Governors on: Feb 2015

2.2 Teaching and learning

2.2.1 Why Internet use is 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.
- 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.

2.2.2 Internet use will 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 given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies 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 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.

2.3 Managing Internet Access

2.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Newcastle LA.
- 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.

2.3.2 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.
- 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 not permitted.

2.3.3 Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupil's work and photographs can only be published with the permission of the pupil and parents.

2.3.4 Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be 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 attended, IM and e-mail address, full names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

2.3.5 Managing filtering

- The school will work with the LA, DCFS and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.6 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils are not allowed mobile phones in school, unless handed to staff for safe keeping.
- If necessary, staff will be issued with a school phone where contact with pupils is required. (see BR for hers or GJ for his).

2.3.7 Protecting personal data

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

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- 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 may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials using PC and IPad. At Keys Stage 2 access will be supervised by staff with all access monitored by the LA filtration and protection system.
- Parents will be asked to sign and return a consent form.

2.4.2 Assessing risks

- 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 Newcastle LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of the management team.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

2.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all class rooms and the ICT suite and discussed with the pupils at the start of each term.
- Pupils will be informed that network and Internet use will be monitored.

2.5.2 Staff and the e-Safety policy

- 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.

2.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and the school brochure.

Headteacher:		Date:
Chair of Governing Body:		Date:

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.
Publishing images, including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.