Arnold View Primary School E-safety Policy

Living, Learning & Achieving Together

Date reviewed: January 2018 **Next review: January 2019**

Signed _____ (Head teacher) **Date: _____**

Signed _____ (Chair of Governors) **Date:_____**

Overview

E-safety encompasses internet technologies and electronic communications such as mobile phones and wireless technologies. The primary focus of e-Safety is safeguarding children. It highlights the need to educate children about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness for users, helping them to develop an understanding of how to keep themselves safe, and control their online experience.

The e-Safety Policy operates in conjunction with other policies including those for ICT, Behaviour, Bullying, Safeguarding and Staff Contact.

Our designated e-Safety coordinator is Denise Bryant.
Our designated ICT coordinator is Denise Bryant (Temporary)
Our designated e-Safety / ICT governor is Mr Key

Any incidents of misuse should be reported to the head teacher (Denise Bryant), or in their absence to the deputy head teacher (Emma Bowler) or school business manager (Kate Padwick). Incidents should be logged on CPOMS.

Teaching and Learning

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 students with quality Internet access as part of their online learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
As pupils use the Internet widely outside of school, they need to be aware of the potential risks and how to avoid them so they may enjoy the benefits of their online world.

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.

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 will regularly model appropriate online behaviours. Staff will oversee all access to the Internet during school time, to ensure learning reflects 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 be taught never to give out personal details of any kind, including usernames and passwords.

Pupils will be taught how to evaluate Internet content:

The school will ensure that the copying and subsequent 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 will be taught what to do if they see any unpleasant Internet content. (AUP guidelines)

Managing Internet Access

Information system security:

Virus protection will be updated regularly.

School ICT systems security will be reviewed regularly.

Security strategies will be discussed with the Local Authority.

E-mail

Pupils may only use approved email accounts. All emails received and sent will be monitored by the class teacher.

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 external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published Content:

The contact details given online will be the school office. Staff or pupils' personal information must not be published.

The headteacher, in conjunction with the office manager, will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work:

Written permission from parents or carers will be obtained before images of pupils are electronically published.

Images that include pupils will be selected carefully. Group photographs of children will be used on the school website, rather than individual photos, where appropriate. Images placed on Twitter must be approved and awareness of parent's requests not to allow their child's picture or detail to be used must be adhered to.

Pupils' full names will not be used anywhere on the website, Twitter and/or school blog, particularly in association with photographs.

Work can only be published online with the permission of the pupil and parents.

Social networking and personal publishing:

The school will block access to social networking sites (through EMBC) and consider how to educate pupils in their safe use.

Twitter must only be used to promote the school and its activities and it must not share confidential data or images.

Pupils will be told never to give out personal details of any kind which may identify them, their friends or their location. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers and risks for primary aged pupils and use of these by pupils should be carefully supervised and monitored at all times.

Managing filtering:

The school will work with EMBC, DfES, and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator or ICT coordinator.

Any material that the school believes is illegal must be reported to appropriate agencies such NCC, IWF or CEOP (http://www.ceop.gov.uk).

Teachers are responsible for making sure checks are made to ensure filtering methods selected are appropriate, effective and reasonable, e.g. running key word searches on Google images, prior to lesson, to check content is appropriate.

Managing video conferencing and webcam use:

IP videoconferencing should use the educational broadband network (EMBC- 'Click to Meet') to ensure quality of service and security rather than the Internet.

Videoconferencing should be supervised appropriately for the pupils' age.

Videoconference calls (making or answering) should always be led by a class teacher.

All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Parents and guardians should agree for their children to take part in videoconferences.

Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Teachers need to 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 the class.

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.

Staff will use a school phone where contact with pupils / parent's is required. (See staff contact policy for more details).

Appropriate use of the school blog will be discussed with children including safe and sensible use of forums and uploading documents / pictures.

Forums will be monitored regularly by all school staff.

Passwords to school blog and emails will be changed yearly and, if recorded must be encrypted and not obvious.

Children are not allowed mobile phones or any other electronic devices within class and any mobile phones brought into school should be given to the school office and collected at the end of each school day.

Protecting personal data:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the new GDPR as of May 2018.

Policy Decisions

Authorising Internet Access:

All staff must read the 'Acceptable Use Policy' (AUP) and e-Safety policy.

The school will maintain a current record of all staff and pupils who are granted access to the school ICT systems.

At Foundation and Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Assessing risks:

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor NCC can accept liability for the material accessed, or any consequences resulting from Internet use.

The school should 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 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.

Handling e-safety complaints:

Complaints of Internet misuse will be dealt with by class teachers in the first instance and logged on CPOMs and members of the SLT informed.

Any complaint about staff misuse must be referred to the Headteacher and in her absence the deputy head teacher.

Sanctions within the school discipline policy include: interview/counselling by the headteacher/DHT/TA; informing parents or carers; removal of Internet or computer access for a period.

Pupils will be informed of the consequences of any misuse on school ICT systems or online school networks.

Discussions will be held with the LA to establish procedures for handling potentially illegal issues.

School staff will continually review forum use and consider how they can best safeguard forums to avoid any further problems.

Parents and pupils will need to work in partnership with staff to resolve issues.

Community use of the Internet:

The school will liaise with family of schools and the LA to establish a common approach to e-Safety.

Communications Policy

Introducing the e-Safety policy to pupils:

E-safety guidelines will be posted in all classrooms.

Safe and sensible use of the Internet will be modelled by adults during whole class teaching, for instance, when using the Internet as a research tool or uploading to the school blog.

Children will be reminded of the e-Safety guidelines prior to supervised Internet access.

Children will be told all computer and Internet use, including classroom blogs, Class dojo and Twitter, is monitored and any misuse will have serious consequences.

E-safety training will be included within the ICT programme of study and PSHE curriculum, raising the awareness and importance of safe and responsible internet use. *(See separate programme list).*

Children will be encouraged to visit the e-safety webpages promoted and click the links to games and activities warning them of the potential dangers and how to make the right online choices.

E-safety parent / pupil agreements will be sent home, within the children's planners to sign.

Staff and the e-safety policy:

All staff will be given the school e-Safety Policy and its application and importance explained. It is their responsibility to ensure they read and follow procedures outlined in it.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. (See staff contact policy).

Staff training will be provided in safe and responsible Internet use.

Enlisting parents' support:

Parents' attention will be drawn to the school's e-Safety guidelines in newsletters, on the school website and in the school brochure.

Internet issues will be handled sensitively and parents will be advised accordingly.

A partnership approach with parents will be encouraged. This could include parent 'meet and greet' sessions at the beginning of each school year with demonstrations and suggestions for safe home Internet use.

Parent/child e-Safety agreements will be sent home annually.

Parents will be informed when email / webcam relationships have been established and their purpose and nature will be explained.