ALPINGTON & BERGH APTON CHURCH OF ENGLAND V.A. SCHOOL

E-SAFETY POLICY

CO-ORDINATOR: Teresa Osborne

APPROVED BY: The Full Governing Body: January 2017

DATE FOR REVIEW: January 2018

Alpington V.A Primary E-Safety Policy

The e-safety policy is part of the School Improvement and Development Plan and relates to other policies including those for ICT, bullying and for child protection.

The school has appointed an e-safety coordinator. This is the designated Child Protection co-ordinator as the roles overlap (headteacher).

- Our e-safety Policy has been written by the school, building on the Norfolk e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The e-safety Policy and its implementation will be reviewed annually.
- The e-safety policy was revised by: Teresa Osborne
- It was approved by the governors: January 2017

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 learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

The school's 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

Pupils will be taught how to evaluate internet content

We will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

- As pupils progress through the school into Key Stage 2 they will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Information System Security

School ICT systems capacity and security will be reviewed regularly in accordance with Becta Framework for IT Support (FITS).

Virus and Spyware protection will be installed and updated regularly.

Security strategies will be discussed with the Local Authority and with the technician attached to our school.

Email

In certain controlled circumstances the pupils may use email with teacher consent:

Pupils may only use approved e-mail accounts, i.e. nsix.org.uk.

Pupils must immediately tell a teacher if they receive offensive e-mails.

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.
- Email subscriptions to websites or other electronic services should be authorised.
- Parents have the option of receiving the bi-weekly newsletter by email providing consent to this is given. School may also use the email account to communicate with parents on other school related matters

NB: At the time of writing pupils are not yet accessing email accounts at school

Published content and the school website

The contact details on the school's web site include the school's address, e-mail and telephone number. Staff or pupils' personal information will not be published.

- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

Written permission from parents is obtained allowing the school to publish photographs of their children in displays, newsletters, school brochures, local newspapers etc and on the school website

Pupils' full names will not be used anywhere on the web site, particularly in association with photographs. **Newsletters will no longer refer to pupils by their full names (27.11. 2015)**

Social networking and personal publishing

The school will work with parents and police via CEOPS to educate children in safe internet use at home and at school

The school will block / filter access to inappropriate 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.

Staff must not communicate with students using public social networking sites such as Facebook, MySpace, Twitter, etc.

Staff should not communicate with parents about school based issues using public social networking sites such as Facebook, MySpace, Twitter, etc. To do so is a disciplinary offence.

The Friends of Alpington Primary school are responsible for running its own Facebook page.

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Mobile Phones and I pads

Mobile phones should not be taken out in classrooms. They may be used in staff only areas such as the staff room or school office. No staff member should have an image of a pupil taken during the school day on their mobile devices.

Staff ipads and laptops may be subject to random security sweeps, this applies to all staff who work regularly at the school.

Personal ipads should not be used for classroom teaching, if they are brought into school they will be subject to school safety procedures.

Personal information on children should not be carried on mobile devices such as memory sticks. No pupil is permitted to use a personal memory stick on school equipment. Staff should be aware that memory sticks used on devices at home can transfer viruses onto the school system. To avoid this Cloud technology should be used instead.

Managing filtering

The school will work in partnership with the LA and E-Safety Group 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 and ICT provider.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

IP (Internet Protocol) videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet, for example using the E2Bn resource, Flashmeeting, where meetings are arranged by the staff on an invitation-only basis. These may be recorded for replay later within further lessons.

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

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, and the view of the Advisory Service and ICT provider shall be sought.

- In the future mobile phones may be used as part of lessons or formal school time. However, at present the school's policy is that children who need to bring in mobile phones (for contact reasons etc) should hand them in to the school office during the day.

Protecting personal data

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

Authorising Internet access

All staff must read and sign the 'Staff code of conduct' before using any school ICT resource. This acts as a current record of all staff and pupils who are granted access to school ICT systems.

- Parents will be asked to sign and return a consent form giving permission for their child to use the internet

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NCC can accept liability for the 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 effective.

Handling e-safety complaints

Complaints of internet misuse will be dealt with by the Headteacher or deputy head.

Any complaint about staff misuse must be referred to the headteacher.

Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.

- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Youth Support Team Inspector, or check out http://www.safernorfolk.co.uk/. to establish procedures for handling potentially illegal issues.

Introducing the e-safety policy to pupils

E-safety rules will be posted in all classrooms where computers are used.

Users will be informed that network and internet use will be monitored.

As they progress through the school, children will be taught these **SMART** tips (from Childnet International – www.childnet.com):

Safe – Keep safe by being careful not to give out personal information – such as your full name, e-mail address, phone number, home address, photos or school name – to people you are chatting with online.

Meeting – Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

Accepting – Accepting e-mails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable – Information you find on the internet may not be true, or someone online may be lying about who they are.

Tell – Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

Staff and the e-safety policy

All staff will be given a copy of the school's 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 or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

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

Parents will be informed about the SMART rules taught to the children in school and will be informed that they may wish to invest in security software for their own computers, e.g:

- Net Nanny, www.netnanny.com
- Cyber Patrol www.cyberpatrol.com
- Surfwatch www.safesurf.com