CHOLLERTON CHURCH OF ENGLAND AIDED FIRST SCHOOL

Be the best you can be through:

challenge, nurture, inspiration, respect, happiness, inclusion, in a safe, loving Christian family.

E-SAFETY POLICY

E-Safety

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, 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 extensively revised and renamed as the 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 Student Behaviour, Bullying, Curriculum, Data Protection, Health & Safety, Safeguarding and Prevent Duty of Care.

End to End e-Safety

- E-Safety depends on effective practice at a number of levels:
- Responsible ICT use by all staff and students; 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 Northumberland LEA.

National Education Network standards and specifications.

School e-safety policy

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

The school will appoint an e-safety Co-ordinator. This may be the Designated Child Protection Co-ordinator as the roles overlap.

- Our E-safety Policy has been written by the school, building on N.C.C. E-safety Policy and government guidance. It has been agreed by senior management and approved by Governors and the P.T.F.A.

  The following national guidelines should also be read when working with this policy:
- Prevent Strategy, HM Government
- Keeping Children Safe in Education, DFE 2018
- Working together to safeguard children, HM Government 2015

- Changes will be made immediately if technological or other developments so require.

- The E-safety Policy and its implementation will be renewed annually

- The E-safety Policy was revised by Mrs H. Davey who is also the Designated Child Protection Co-ordinator.

- It will be presented to the Governors for review in October 2018 at the Autumn Governor's meeting.
  .

1. Teaching & 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 learning experience.
- 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students, they need to show a responsible and mature approach to its use.
- 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.

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.

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

How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC);
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services, professional associations and between colleagues;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to tools of direct communication, including video conferencing and e-mail.
- Exchange of curriculum and administration data with N.C.C.

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.

2. Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

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.

Published content and the school website

- The contact details on the Website should be the school 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.
- At present, editorial responsibility for all other areas of website is jointly held by: Mrs H Davey and Mrs K Adshead.
- The website should comply with the school's guidelines for publications.
- The copyright of all materials must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Publishing Photographs

- Pupils' full names will not be used anywhere on the website or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- Social networking and personal publishing is not permitted in school.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA, DfES and the Internet Service provider to ensure systems to protect pupils are reviewed and if staff or pupils discover an unsuitable site, it must be reported to the e-safety co-ordinator, who will inform the Internet Service provider.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will be appropriately supervised for the pupils' age.
- Parental permission will be sought for children to take part in videoconferences.
- Only key administrators should be given access to videoconferencing systems, web or other remote control page.
- Unique log on and password details for the educational videoconferencing service should only be issued to members of staff and kept safe.
- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Recorded material shall be stored securely.
- Preparation and evaluation are essential to the whole activity.
- 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 your 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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

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

3. Policy Decisions

Authorising Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All staff and pupils will initially be granted Internet access.
- All staff and pupils have authenticated passwords and logins to access the computers and the Ipads.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form.
- Pupils will not be allowed to use computers with Internet unless they are directly supervised by a member of staff.
- Guidelines relating to Internet safety are visible from all machines with Internet access, throughout the school.

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 N.C.C. 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.
- 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.
- The Headteacher will ensure that the e-safety policy is implemented and compliance with the policy monitored.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- 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.

Community use of the Internet

- The school will liaise with the local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, and offer appropriate advice, e.g. appropriate websites to use with First School children.

4. Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all rooms and discussed with the pupils throughout the school year.

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 used.
- Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-safety policy in newsletters, the school brochure, school website and at Parent information events.
- A partnership approach with parents will be encouraged. This will include leaflet distributions, demonstrations, practical sessions and suggestions for safe Internet use at home.

Approved by the Governing Body:

Signed by -

.....

This policy was reviewed: **Autumn 2018**
Date of next review: **Autumn 2020**

Appendix 1

Internet use – Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
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.	