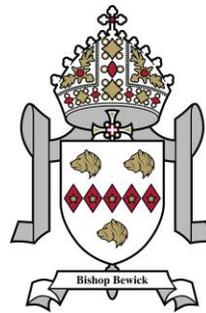


St Cuthbert's Catholic Primary School Walbottle



E-Safety Policy

At St Cuthbert's we live and learn in faith and love,
through Jesus's teachings.

Our school is a place where we can grow as a family,
helping each other to lead full and happy lives.

Consultation that has taken place	
Date Formally Approved By Governors	23.06.2021
Date policy Became Effective	24.06.2021
Review Date	June 2022
Person Responsible for Implementation and Monitoring	HT Govs

Introduction

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.

End to End e-Safety

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

- Responsible use of computing equipment 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 the Newcastle network including the effective management of filtering.

Further Information

IT Assist – Dave Punton

07828971064

Newcastle ICT staff

0191 2777282

E-Safety Audit

This quick self-audit will help the senior management team (SMT) 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 guidance?	Y
Date of latest update: April 2021	
The Policy was agreed by governors on: April 2021	
The Policy is available for staff on the staff server	
And for parents at: The school website	
The Designated Child Protection Coordinator is: Mrs Barrett	
The e-Safety Coordinator is: Miss Gallagher	
Has e-safety training been provided for both students 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?	Y
Have school e-Safety Rules been set for students?	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 DfES requirements for safe and secure access	Y
Has an ICT security audit has been initiated by SMT, possibly using external expertise?	N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

2.1 Writing and reviewing the 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 Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on the National Curriculum and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed every two years.
- The e-Safety Policy was revised by:
- It was approved by the Governors on:

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 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 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

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

Managing Internet Access

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.

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 web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site 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 Web site.

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.
- 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, DfE 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.

Managing video conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age .
- The School will use Microsoft teams or Zoom to conduct video calls.
- A Code of Conduct for Teams and Zoom is signed by all staff.

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 and smart watches will not be used/worn 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.

Policy Decisions

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.

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 NCC 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.

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 Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

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.

Enlisting parents' support

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

This policy was approved by the Governing Body on

Signed

