St Mary's Catholic First School

E-Safety Policy 2022 - 23

Bishop Wilkinson
Catholic Education Trust
Through Christ, in Partnership

Part of the Bishop Wilkinson Catholic Education Trust
Company Registration Number 07890590

Chair of Governors	**Mark Dotchin**
Headteacher	**Sarah Oakes**
Review Period	**Sept 2022**
Next Review Date	**Sept 2023**

E-Safety

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, mobile devices, 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 purpose of the e-Safety Policy is 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 and Security.

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 the Northumberland County - Network including the effective management of filtering.
- National Education Network standards and specifications

Writing and reviewing the E -safety policy

Our e-Safety Policy has been written by the school, building on Government guidance. It has been agreed by senior management and approved by governors and the FOSM. The e-Safety Policy and its implementation will be reviewed annually.

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 children

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.

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 allocated a particular computer so monitor can be safe and secure.

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 Northumberland County Council.

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 Web site 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

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 Website.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites (blocked by LA)
- 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 on the website/ parent evenings etc.

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

Managing videoconferencing

- 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.

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.

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, change in planning.

At Key Stage 1 and 2, access to the Internet will be by adult demonstration and directly supervised with access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form.

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 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. - Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet Introducing the e-safety policy to pupils

- E Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and constantly throughout
- 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 newsletter, the school brochure and on the school website.

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.	Web directories e.g. Ikeep bookmarks Webquest UK Northumberland Grid for Learning
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.	Web quests e.g. - CBBC Search
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.	RM EasyMail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
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.	Making the News SuperClubs Infomapper Headline History Northumberland Grid for Learning Focus on Film
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.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or	Only chat rooms dedicated to educational use and that are moderated	

online forums.	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.	FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum

St Mary's RC First School

ACCEPTABLE USE BY STAFF OF ICT SYSTEMS IN SCHOOL

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher. This includes PCs and data.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will ensure that any images that are stored will be removed as soon as they are no longer required.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will ensure that my computer is locked or switched off whenever I leave my device.
- I will ensure that my computer is switched off at the end of the day.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

ACCEPTABLE USE OF SCHOOL E-MAIL ACCOUNTS

- I am responsible for the use of my device. I will ensure that other family members do not have access to data and e-mails.
- I will ensure that all sensitive e-mails containing identifiable data will be stored in a separate folder.
- I will only save attachments with personal data on school equipment.

ACCEPTABLE USE OF MOBILES, SMART WATCHES AND MOBILE DEVICES

- I will switch off my mobile during the working day.
- I will not use my mobile or any other personal device for taking photographs in school.
- I will not use my mobile or any other personal device for communication with parents.
- I will ensure that any engagement in any online activities does not compromise my professional responsibilities.

ACCEPTABLE USE OF SOCIAL MEDIA

- I will have no contact with pupils or their siblings even when they have left school.
- If I am in contact via social media with any current or past parents I will declare it in writing to the Executive Headteacher and Governors.
- I will not mention the school by name or in passing, or discuss individuals or groups within the school, or compromise the school values.
- I will use the highest possible privacy settings.
- I will be aware that I may be 'tagged' in other photographs.
- I will not post or comment on anything that may be libellous or bring the school into disrepute. The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

  A failure to comply with any of the above may result in disciplinary action.

I have read, understood and agree with the Acceptable use policy.

Name: ……..... Signature: …….…… Date: ……..