Cardinal Newman Catholic High School in Warrington

eSafety Policy

eSafety Policy

Introduction

Where we use the terms 'e-safety' or 'online', we refer to all fixed and mobile technologies which children and young people might encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks to their wellbeing and safety.

eSafety encompasses the use of new technologies, internet and electronic communications, publishing and the appropriate use of personal data. 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 school's eSafety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

Students benefit from internet use by:

- Access to world-wide educational on line resources and virtual tours such as religious buildings, museums and art galleries

- Access to online curriculums in other schools

- inclusion in government initiatives and web sites

- educational and cultural exchanges between students world-wide;

With all technologies there are risks as well as benefits. It is vital that the students in our care schools adopt strategies for the safe and responsible use of new technologies.

Directed educational use

The Internet can be used to access to information from around the world, communicate widely and to publish work easily. School Internet use should be planned, task-orientated and educational within a regulated and managed environment.

Preventing dangers

In school it is necessary to protect students from websites containing inappropriate materials. Students are protected in the main from such material by LEA and school based filtering, which identifies inappropriate material in advance and blocks these sites. Students are required to inform a member of staff if they come across any unsuitable material. If staff or students discover unsuitable sites, the URL (address) and content must be reported to a member of staff and also inform the network manager who will block the site.

Responsibility

The E-safety policy requires students to take responsibility for the use of Internet and other communication technologies such as phones and video equipment. Mobile phones are not allowed to be used in school without specific permission for a particular use from a member of staff. (Digital equipment policy).. There are no foolproof solutions, staff and students must remain vigilant.

eSafety Policy

End to End eSafety

eSafety depends on effective practice at a number of levels:

- Responsible use of the Internet and other communication technologies by all staff and students; encouraged by education and made explicit through published policies.

- Sound implementation of eSafety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband from Warrington including the effective management of filtering.

- National Education Network standards and specifications.

Regulation

Some aspects of the internet, such as chat rooms, social networking sites and forums are completely banned in school due to the immediate dangers that they pose. The network manager will ensure that the filtering methods selected are appropriate, effective and reasonable.

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.

Teaching and learning

The school will make safe internet use a priority and will where appropriate use materials from organisations such as CEOP, Safer Internet Day etc. to support pupil online safety and to raise parental awareness.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Students are 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.

Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Students are 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.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority ICT staff.

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 headteacher or nominee 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 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 Web site.
- Work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- School will block 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 must not place personal photos on any social network space.
- 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.

Managing filtering

- The school will work in partnership 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 eSafety Coordinator or the Network Manager.
- 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.
- Staff will use a school phone where contact with pupils is required.

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 the "Acceptable ICT Use Policy for staff" before using any school ICT resource.
- Students must agree to comply with the Responsible Internet Use statement.

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 WBC can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate.

Handling eSafety 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
- External organisations using the school's ICT facilities must adhere to the eSafety policy.

Communications Policy

Introducing the eSafety policy to pupils
- eSafety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the eSafety policy
- All staff will be given the School eSafety 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 eSafety Policy in newsletters, the school brochure and on the school Web site.

Writing and reviewing the eSafety policy

The eSafety 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 eSafety coordinator. In many cases this will be the Designated Child Protection Coordinator as the roles overlap.
- Our eSafety Policy has been written by the school, building on the Warrington eSafety Policy and government guidance. It has been agreed by senior management and approved by governors and the PTA.
- The eSafety Policy and its implementation will be reviewed annually.
- The eSafety Policy was reviewed by: … Amc Sept 2014
- It was approved by the Governors on: …Oct 2013

Cardinal Newman Catholic High School

eSafety Policy

eSafety Audit

This quick audit helps the senior management team (SMT) assess whether the basics of eSafety are in place.

The school has an eSafety Policy that complies with Warrington guidance.	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at	
And for parents at	
The Designated Child Protection Coordinator is	
The eSafety Coordinator is	
How is eSafety training provided?	
Is the Think U Know training being considered?	Y/N
All staff will be provided with an Acceptable ICT Use Agreement on appointment.	Y/N
Parents agree that their child will comply with the school Acceptable ICT Use statement.	Y/N
Rules for Responsible Use have been set for students:	Y/N
These Rules are displayed in all rooms with computers.	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	Y/N
The school filtering policy has been approved by SMT.	Y/N
An ICT security audit has been initiated by SMT, possibly using external expertise.	Y/N
School personal data is collected, stored and used according to the principles of the Data Protection Act.	Y/N
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SMT.	Y/N

Cardinal Newman Catholic High School

eSafety Policy