

St Benedict's Catholic High School – E-Safety Policy – March 2010

- *Our e-Safety coordinator is Mrs M Deeks who will share the role with the Designated Safeguarding Coordinator, Mrs C Wilks, as the roles overlap.*
- *Our e-Safety Policy has been written by the school, building on the Warwickshire ICT Development Service e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors and the PTA.*
- *The e-Safety Policy will be reviewed annually.*

Teaching and learning

Why Internet use is important

- *Internet use is part of the statutory curriculum and a necessary tool for learning.*
- *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 information and business administration systems.*
- *Internet access is an entitlement for students who 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.*

How does Internet use benefit education?

Benefits of using the Internet in education include:

- *Access to world-wide educational resources including museums and art galleries;*
- *Inclusion in the National Education Network which connects all UK schools;*
- *Educational and cultural exchanges between pupils world-wide;*
- *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 and professional associations;*
- *Improved access to technical support including remote management of networks and automatic system updates;*
- *Exchange of curriculum and administration data with the LA and DfES;*
- *Access to learning wherever and whenever convenient.*

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.*
- *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.*

Pupils will be taught how to evaluate Internet content

- *If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service, and where appropriate the school e-safety officer.*
- *Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.*

The following statements require adaptation according to the pupils' age:

- *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 taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.*
- *The evaluation of on-line materials is a part of every subject.*

Managing Internet Access

Information system security

- *The security of the school information systems will be reviewed regularly.*
- *Virus protection will be installed and updated regularly.*
- *The school uses the Warwickshire Broadband with its firewall and filters.*
- *The school provides an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Service.*
- *Portable media may not used without specific permission and a virus check.*
- *Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail, or on any other portable media.*
- *Files held on the school's network will be regularly checked.*
- *The ICT co-ordinator/network manager will review system capacity regularly.*

E-mail

Pupils and staff are expected to adhere to the generally expected rules of network etiquette (netiquette) . These include but are not limited to the following:

- Be polite.
- Use appropriate language.
- Do not get abusive in your messages to others.
- Do not reveal the personal address, phone number or other personal details of yourself or other users.
- Do not use the network in such a way that would disrupt the use of the network by other users.
- Illegal activities are strictly forbidden.
- Note that e-mail is not guaranteed to be private.
- System administrators have access to all mail.
- Messages relating to or in support of illegal activities may be reported to the authorities.

- *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.*
- *Use of words included in the Policy Central 'banned' list will be detected and logged.*
- *Access in school to external personal e-mail accounts may be blocked.*
- *Excessive social e-mail use can interfere with learning and may be restricted.*
- *E-mail sent to external organisations 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 Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.*
- *Email addresses should be published carefully, to avoid spam harvesting.*
- *The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.*
- *The Website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.*

Publishing staff and 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, 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.*
- *Pupil's work can only be published with the permission of the pupil and parents.*
- *Images of staff should not be published without consent.*

Social networking and personal publishing

- *Social networking sites and newsgroups will be blocked unless a specific use is approved.*
- *Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.*
- *Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.*
- *Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for students on a personal basis.*
- *Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.*
- *Students should be advised not to publish specific and detailed private thoughts.*
- *Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.*

Managing filtering

- *The school will work in partnership with the Warwickshire ICT Development Service and Becta to ensure filtering systems are as effective as possible.*
- *If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.*
- *We will manage the configuration of our filtering. This task requires both educational and technical experience.*
- *Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.*
- *Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP (addresses later).*

Managing videoconferencing

The equipment and network

- *All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.*
- *IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.*
- *Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.*
- *External IP addresses should not be made available to other sites.*
- *Videoconferencing contact information should not be put on the school web site.*
- *The equipment must be secure and if necessary locked away when not in use.*
- *School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.*

Users

- *Pupils should ask permission from the supervising teacher before making or answering a videoconference call.*
- *Videoconferencing should be supervised appropriately for the pupils' age.*
- *Parents and Guardians should agree for their children to take part in videoconferences, probably in the annual return.*
- *Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.*
- *Only key administrators should be given access to the videoconferencing system web or other remote control page available on larger systems.*
- *Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.*

Content

- *When recording a lesson, written permission should be given by all sites and participants. The reason for the 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.*
- *If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).*
- *Videoconferencing is a challenging activity with a wide range of learning benefits. 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.*
- *The school will investigate cellular wireless, infra-red and Bluetooth communication and decide a policy on phone use in school.*
- *Staff should be issued with a school phone where contact with pupils is required.*

Protecting personal data

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual). The act also gives rights to the people the information is about i.e. the right of subject access, lets individuals find out what information is held about them.

The eight principles are that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Held no longer than is necessary
6. Processed in line with individuals rights
7. Kept secure
8. Transferred only to other countries with suitable security measures.

The Information Commissioner's Office provides relevant information:
<http://www.ico.gov.uk/>

- *Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. See Fair Processing notice on school website (check)*

Policy Decisions

Authorising Internet access

- *The school will maintain a current record of all staff and pupils who are granted Internet access.*
- *All users must read and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource.*
- *Secondary students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.*

Assessing risks

- *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 WCC can accept liability for the material accessed, or any consequences of Internet access.*
- *The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.*
- *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.*

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 who should use the agreed WCC procedures.*
- *Pupils and parents will be informed of the complaints procedure.*
- *Parents and pupils will need to work in partnership with staff to resolve issues.*
- *Sanctions within the school discipline policy include:*
 - *interview/counselling by head of year;*
 - *informing parents or carers;*
 - *detentions;*
 - *removal of Internet or computer access for a period.*

Community use of the Internet

- *The school will liaise with 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, e.g. social networking sites, and offer appropriate advice.*
- *All members of the school community will be made aware of the school policies for internet use and e-safety.*

Communications Policy

Introducing the e-safety policy to pupils

Useful e-safety websites include:

- Think U Know; currently available for secondary pupils. Primary based materials will be available September 2007 (www.thinkuknow.co.uk)
 - SuperClubs (ex. GridClub) www.superclubsplus.com/
 - Internet Proficiency Scheme www.gridclub.com
 - The BBC's ChatGuide www.bbc.co.uk/chatguide/
 - CBBC Stay Safe www.bbc.co.uk/cbbc/help/safesurfing/
-
- *Rules for Internet access will be posted in all networked rooms.*
 - *Pupils will be informed that Internet use will be monitored.*
 - *An e-Safety training programme is carried out to raise the awareness and importance of safe and responsible Internet use.*
 - *Instruction in responsible and safe use should precede Internet access.*
 - *A module on responsible Internet use will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.*

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 and other computer use can be monitored both in school and away from school on equipment provided by the school and traced to the individual user. Discretion and professional conduct is essential.*
- *All staff should read and abide by an Acceptable ICT Use Policy.*
- *Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.*
- *Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.*

Enlisting parents' support

- *Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Website.*
- *Internet issues will be handled sensitively to inform parents without alarm.*
- *Using our triangle of communication between staff, parent and pupil a partnership approach with parents will be encouraged. This could include parents' evenings with demonstrations and suggestions for safe home Internet use.*
- *Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.*
- *Interested parents will be referred to organisations listed e-Safety Contacts and References, listed below.*

e-Safety Contacts and References

Child Exploitation & Online Protection Centre

http://www.ceop.gov.uk/contact_us.html

Think U Know website

<http://www.thinkuknow.co.uk/>

Kidsmart

<http://www.kidsmart.org.uk/>

Childline

<http://www.childline.org.uk/>

Stop Text Bully

<http://stoptextbully.com>

CBBC Safe Surfing including the Chat Guide

<http://www.bbc.co.uk/cbbc/help/safesurfing/>

Parents' Centre

<http://www.parentscentre.gov.uk/usingcomputersandtheInternet/>