§II-7002.7 Internet Safety

II-7002.7 ***Policy***

The Diocese of Davenport recognizes and promotes the increasing availability of Internet access in schools and parishes throughout the Diocese. The Internet is an electronic highway connecting thousands of computers all over the world with access to electronic mail, public domain software, discussion groups, libraries of information and other forms of direct electronic communication.

Along with the inherent freedom of the Internet comes the possibility of accessing material that is not consistent with the Catholic faith. Although precautions should be taken to restrict access to controversial materials, such access may still be possible.

Procedures

To safeguard the Internet and its users the Diocese requires that the following regulations be enforced by the system administrators of each Internet access site in the Diocese:

a) Transmission or intended reception of any material in violation of any national, state or local regulation is prohibited. This includes, but is not limited to: copyrighted material (without appropriate permission), threatening or obscene material or material protected by trade secret. Use for commercial activities, product advertisement, or partisan political lobbying is prohibited. Intended transmission or reception of materials that would tend to violate the moral teaching of the Catholic Church or be scandalous to the Church is also prohibited. Any child pornography discovered shall be reported to law enforcement authorities and the offender removed from ministry.

b) Any network or computer may be monitored for improper use, network diagnosis and virus detection.

c) The Diocese requires the use of filtering software or services on all school computers with access to the Internet. This particular filtering and monitoring may also be done on all other computers without previous notice. Computers and networks that access the Internet must maintain a firewall that limits access to required services. Firewall and wireless access points shall not use vendor-supplied defaults for system passwords and other security parameters. Network logging is maintained. Security assessments shall be performed on a regular basis to ensure network integrity.

d) When minors are using the Internet, access to visual depictions must be blocked or filtered if they are (a) obscene, as that term is defined in section 1460 of title 18, United States Code; (b) child pornography, as that term is defined in section 2256 of title 18, United States Code; or (c) harmful to minors. Staff may not disable the filters when minors are using them, even with parental or teacher permission and supervision. Appropriate staff may disable filters only for adults who are using filtered computers for bona fide research purposes. Minors' use of the Internet should be monitored. Appropriate language shall be used while respecting the rights of others. Diocesan entities shall abide by the federal *Children's Online Privacy Protection Act* (COPPA).

e) Appropriate language shall be used while respecting the rights of others. The USCCB Code of Conduct should be posted on all social networking sites: "All posts and comments should be marked by Christian charity and respect for the truth. They should be on topic and presume the good will of other posters. Discussion should take place primarily from a faith perspective. No ads please." Social networking sites should be monitored by an adult who shall report violations of the Code of Conduct to the appropriate staff.

f) In general, personal addresses and personal phone numbers should not be made public over the Internet without special permission. Personal addresses and phone numbers of minors should never be given out over the Internet. Illegal activities should be reported to law enforcement.

g) Internet information is not guaranteed to be confidential. The transmission of credit card information and personal identifiable information is prohibited unless a secure system of encryption is used.

h) Attempts to disrupt the use of the network by destroying data of another user or of the network is prohibited. Attempts to use system administrator access rights or another user's account without written permission are prohibited. Any user identified as a security risk may be denied access to the network.

i) All computers should continuously run anti-virus/malware software while in operation. Computer equipment used in home offices that exchange data with Diocesan or Diocesan entity computer networks shall use anti-virus/malware software approved by the Diocesan Director of Technology. Any information downloaded from the Internet should be scanned for viruses before use. Computers and network equipment should utilize current service pack or firmware versions with all applicable current security patches installed.

j) The Diocese of Davenport makes no warranties of any kind, whether expressed or implied, for Internet service including loss of data, delays, non-deliveries, miss-deliveries or service interruptions. Use of any information obtained is at the operator's risk. It is up to the user to verify or validate all of the information obtained. Users are responsible for backing up data not stored on the network.

k) Diocesan entities are required to follow the Social Media Guidelines provided by the USCCB.

l) Employees and adult volunteers shall avoid e-mailing minors using addresses not associated with the diocesan entity. They shall limit messaging with minors to professional purposes only. Great care should be exercised when communicating with minors outside of school hours and away from school-sponsored events and must be for good cause. Parents and guardians must be provided access all messages to minors either by copies of or inclusion in messages.