Technology and Internet Safety and Acceptable Use Policy

Adapted from the Diocese of Davenport

The Diocese of Davenport and John F. Kennedy Catholic School recognize and promote the increasing availability of Internet access in schools and parishes throughout the diocese.

The use of technology in education comes with a corresponding responsibility. 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.

To safeguard the Internet and its users the Diocese and John F. Kennedy Catholic School require that students and employees follow these rules:

1. Users should only be accessing Internet sites and content as related to the educational objectives for which access is deemed appropriate and relevant. All copyright laws must be respected. For example, users must cite all quotes, references, sources, etc. in any report.

2. 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
- threatening or obscene material
- material protected by trade secret

Use for commercial activities, product advertisement, or political lobbying is prohibited.

Intended transmission or reception of material that would tend to violate the moral teaching of the Catholic Church or be scandalous to the Church is also prohibited.

3. The Diocese requires the use of filtering software or services on all school computers with access to the Internet. 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 2256 of title 18, United States Code
c. harmful to minors

Schools cannot disable the filters when minors are using them, even with parental or teacher permission and supervision. Appropriate school staff may disable filters only for adults who are using school computers for bona fide research purposes.

Schools must monitor minors' use of the Internet in school. Parents are responsible for directly supervising and monitoring student Internet access if school owned devices are taken home. The school's filtering software must be run on all school owned devices regardless of location of the device. The school may also act on phrases and searches flagged by the software.

4. Appropriate language shall be used while respecting the rights of others. Messages, documents, and other files shall not contain profanity, obscene or sexually explicit pictures or comments, or expressions of bigotry or hatred.

5. In general, it is advised that personal identification information should not be made public over the Internet. Personal identification of minors, including addresses and phone numbers should never be given out over the Internet. Illegal activities may be reported to law enforcement.

6. Unauthorized access, including so called "hacking" and other unlawful activities online are prohibited. Attempts to disrupt the use of the network by destroying data of another user or of the network or interfering with another user's access to the data are prohibited. Attempts by minors to use system administrator access rights or another user's account without written permission from the school are prohibited. Any user identified as a security risk may be denied access to the Internet or to school computer equipment. Changing the configuration of the school computers, which might include the downloading of games, is prohibited.

7. All computers should continuously run anti-virus software while in operation. Any information downloaded from the Internet should be scanned for viruses before use.

8. The Diocese of Davenport and JFK make no warranties of any kind, whether expressed or implied, for Internet service including loss of data, delays, nondeliveries, mis-deliveries or service interruptions. Use of any information obtained is at the operator's risk.

9. Students will not be allowed to use personal accounts or send or receive e-mail from a home or AHS communications account while at school. Students will not be allowed to use chatrooms, instant messaging, and other forms of direct electronic communication, except for those provided directly by the school for educational purposes. Misuse off our campus may be subject to the discipline policy as well.

All school policies apply to students using accounts on school-provided resources (such as Google Apps for Education, online textbook websites, etc.) regardless of location or time of day. Students may not use school provided accounts and resources to conduct personal conversations unrelated to educational purposes.

Students are responsible for their school-provided accounts and should take all reasonable precautions to prevent others from being able to use their accounts. Students should not provide their passwords to anyone other than their parents or a school employee.

School-provided student accounts are intended for educational purposes only and can be accessed by school administration at any time. The school maintains the right to immediately suspend any school-provided student account if violations of school policies are suspected. In such cases, the alleged violation will be referred to school administration for further investigation.

10. Viewing of Internet information and any posting of content is considered a public act if using school accounts or equipment. There should be no expectation of privacy. School officials may monitor and inspect all usage.

11. Because the information on the Internet is so widespread and constantly changing, it is impossible to predict everything students might locate. Even with teacher supervision, a student may encounter inappropriate information. Students will be instructed on the appropriate use of the Internet, including how to immediately back out of objectionable areas. Students intentionally accessing such information, encouraging others to do so, or failing to immediately back out of accidental encounters will be subject to the consequences listed in the Acceptable Use Policy.

12. Students may be assessed a fee for damages or loss of computer equipment and accessories.

    If computer equipment or accessories are damaged but repairable, the student's family is responsible for the cost of the materials needed to make the repairs. If the computer equipment or accessories are damaged and not repairable or lost, the student's family is responsible for the replacement cost.

    Students must keep food and drinks away from computer equipment. Students must follow any instructions from their teachers on keeping their computer equipment safe and ready for use (storage, handling, using protective cases, recharging, etc.)

    Students must report any damage or lost computer equipment to their teacher as soon as possible. Failure to return a school owned device by the established due date will be considered loss of the device.

13. All school policies apply to students when using school equipment regardless of location and time of day.

14. If students are allowed to take school owned devices home and they forget to bring them back, they may be able to borrow other students' devices with adult permission and pending availability.

15. Students may not borrow another student's computer without permission from a teacher.

16. Students will receive education about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

17. Students are prohibited from accessing the Internet using personal mobile Internet services through their own Internet Service Provider (e.g., mobile Internet services on cell phones, tablets, etc.). CIPA laws require schools to filter students' Internet access and block inappropriate content from being accessed by students when in the building.

18. Unauthorized use of a computing device and taking a photograph or video/audio recording without permission is subject to the discipline policy (540.1).

19. No student owned electronic device may be connected to the school's network without permission from the school.

20. Users accessing Internet services that have a cost will be responsible for payment of those costs.

21. The contents of this policy, except for the insurance elements, also apply to students who are using Assumption provided machines.

If the user violates any of these provisions, their Internet and/or computer access may be restricted and future access may be denied.

TECHNOLOGY AND INTERNET SAFETY AND ACCEPTABLE USE POLICY VIOLATIONS-CONSEQUENCES & NOTIFICATIONS

Students who violate this policy shall be subject to the following:

A verbal and written notice will be issued to the student on the prescribed form. The student may lose computer and/or Internet access for a period of time which could include the rest of the school year and/or face other consequences in accordance with the Discipline Policy, depending upon the nature and severity of the offense. Staff members, in consultation with administrators, or administrators will determine the consequences. A copy of the written notice will be provided to the student's parent/guardian and kept in a file by the administration.

Policy Adopted: 1999
Policy Reviewed: June 6, 2000;
Policy Revised: March 5, 2002; June 5, 2007; May 4, 2010; May 1, 2012; May 7, 2013; May 5, 2015; June 6, 2017; June 14, 2018; June 4, 2019; August 4, 2020; June 21, 2021; June 14, 2022; June 6, 2023; August 6, 2024