Network Access and Acceptable Use

Introduction
The culture of Archbishop Stepinac High School (hereinafter “Stepinac”) relies on computer technology and electronic devices as an important resource tool for the students’ education. Technology includes, but is not limited to, computers, tablets, cell phones, computer networks, the Internet and electronic mail. The Acceptable Use Policy is designed to set a framework for responsible and ethical use of technology, protecting the privacy and ensuring the safety of our students and teachers. The Acceptable Use Policy applies to all technology resources brought onto campus. It is each student’s responsibility to follow the guidelines for appropriate and acceptable use.

Philosophy
Access to Stepinac’s computer network and Internet enables students to access their digital textbooks; explore libraries, databases, web pages, and other online resources; and exchange information / communicate with people around the world. Stepinac expects its instructional staff to blend thoughtful use of educational technologies and the Internet throughout the curriculum to improve instruction and learning, and to provide exemplary guidance to students about responsible digital citizenship.

Educational Purposes
Stepinac provides access to its network and computer technologies to its students specifically for educational purposes. Students are expected to use Stepinac’s network and computer technologies to support classroom activities, perform educational research and/or gather college and career information. Misuse of Stepinac’s network and computer technologies may lead to discipline of the offending student. Stepinac reserves the right to restrict access to its network or computer technologies for educational or safety reasons.

Content, Filtering and Protection
In accordance with the The Child Online Protection Act (COPA), Stepinac educates its staff and students regarding appropriate online behavior, including use of email and other online resources, to ensure Internet safety. Stepinac has also deployed firewalls, filtering technology and other protection measures to restrict access to inappropriate content such as those that are illegal, obscene or harmful to minors. While every effort is made to provide the most secure and optimal learning environment, it is not possible to absolutely prevent access (accidental or otherwise) to inappropriate content. If you come across any inappropriate content or communication notify an administrator and/or the Technology Office immediately. Students may make written requests to the Technology Office if they believe the content filter is blocking access to appropriate sites.

Consequences of Violation of These Terms
If reasonable belief exists that the student has violated the terms of this agreement, or other

school policy, the student's device may be inspected and/or confiscated. Subsequent or additional disciplinary action involving misuse of technology may also extend to restricted access to Stepinac's network, loss of technology privileges and/or further disciplinary action as determined by the school.

Guidelines for Appropriate and Acceptable Use of Technology

1. Students may ONLY use Stepinac's filtered wireless network to access the Internet while on school grounds. Use of hotspots, VPNs or other wireless networks (e.g., optimum- wifi, xfinity-wifi, cellular data) is strictly prohibited.

2. Students must only use their own electronic device and must only open, view, modify, and delete their own computer files. Use of another student's device, no matter how short, is prohibited.

3. Students will be assigned individual email and network accounts and must use only those accounts and passwords that they have been granted permission to use. All account activity should be for educational purposes only.

4. Students MUST only use their stepinac.org email address when communicating with all Stepinac faculty and staff members.

5. Internet use in the classroom must be directly related to school assignments and projects.

6. Use of electronic devices during class is solely at the teacher's discretion. Students must keep devices turned off and put away when not directed to use them.

7. Students must immediately report threatening messages or discomforting Internet files/sites to a teacher, counselor, administrator or the Technology Office.

8. Students are responsible at all times for their use of Stepinac's electronic communications system, including email, wireless network access, and digital tools/resources, and must assume personal responsibility to behave ethically and responsibly.

9. Students will not vandalize, damage, disable or hack into any electronic technology or system used by Stepinac.

Summary of Acceptable Use

- Stepinac defines acceptable educational use as activities that directly or indirectly support the educational activities of students' classes.
- Stepinac defines acceptable personal use during lunch or study as reasonable and limited personal communication or recreation, such as reading or game playing.
- Students may use their device to access the following resources: email, calendars, contacts, educational documents, sanctioned books and sanctioned educational sites.

- Students are blocked from accessing certain websites while connected to the Stepinac network in accordance with The Child Online Protection Act (COPA)
- Devices' camera and/or video capabilities are not disabled while on-site. Devices may ***not*** be used at any time to:

    - Store or transmit illicit materials
    - Store or transmit proprietary information belonging to another student or teacher
    - Harass others
    - Engage in outside business activities
    - Share homework, exam questions/answers, labs or assignments that are assessed for class academic standing (i.e. group chats, photos, messages boards, etc.)
    - Use or download websites or apps that provide answers to Pearson texts and other assessments.
    - § Apps/websites not conducive to the students' learning experience are blocked at the discretion of the administration of Archbishop Stepinac and are not permitted, including but not limited to:
        - Social media (ie Facebook, twitter, Instagram, snapchat)
        - Any containing illicit or inappropriate material
        - Itunes
        - Google Play
        - Group chats and websites that promote sharing of answers, plagiarism, etc.

Inappropriate Uses

The following uses of technology and actions are prohibited on Stepinac's networks and on school grounds:

1. Using Stepinac's networks and/or communications system for any illegal purposes including, but not limited to: cyberbullying, gambling, pornography, and computer hacking.

2. Disabling or attempting to disable or bypass any system monitoring or filtering/security measures, including the use of VPNs, proxy servers, and wireless networks/hotspots not provided by Stepinac.

3. Tampering with, modifying or changing any system software, hardware or wiring or taking any action to violate Stepinac's security system.

4. Deliberately attempting to degrade or disrupt equipment, software or system performance by spreading computer viruses, engaging in "spamming" or by any other means.

5. Using Stepinac's network in such a way as to disrupt the use of the system by other users. This includes, but is not limited to, using an excessive amount of the network's bandwidth (e.g. by streaming videos, playing online games, etc.).

6. Using the camera feature to capture, record, or transmit audio, video or still photos of other students, faculty, or staff without explicit permission given by a teacher AND all subjects of the photo or video

7. Attempting to access any pornographic, obscene or sexually explicit material.

8. Attempting to log in through another person's account, or use computer accounts, access codes or network identification accounts other than those assigned to the user.

9. Sharing user names and passwords with others.

10. Purposefully opening, viewing, using or deleting files belonging to another system user without permission.

11. Downloading or plagiarizing copyrighted information.

12. Accessing answers to assessments or assignments.

13. Electronically posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

14. Attempting to gain unauthorized access to restricted information or network resources.

15. Posting, using and/or storing personal and confidential information about another person (including but not limited to: home address, phone number, etc.) in any electronic communication form including, but not limited to: emails, text messages, public websites and/or social media sites.

Privacy & Security

Users should have no expectation of privacy when using Stepinac's network and/or equipment. Stepinac reserves the right to periodically and routinely monitor and/or record all communications which use its network for the purposes of network security and student safety. These communications include, but are not limited to: all Internet traffic to and from a student's device while using Stepinac's wireless network; all e-mail communications sent or received through the student's stepinac.org account (whether sent/received on school grounds or elsewhere); and all files stored on the student's stepinac.org cloud drive.

Disclaimers

1. Stepinac cannot be held accountable for the information that is retrieved via the network.
2. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

3. Stepinac will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or your errors or omissions. Use of any information obtained is at your own risk.
4. Stepinac makes no warranties (expressed or implied) with respect to:
    a. the content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information; and
    b. Any costs, liability, or damages caused by the way the user chooses to use his or her access to the network.
5. Stepinac reserves the right to change its policies and rules at any time.
6. Stepinac reserves the right to publish school photographs of students or samples of student's work stored on the network on its website unless express permission is denied in writing by a student's parent or guardian.