St Elizabeth Ann Seton Catholic School
TECHNOLOGY ACCEPTABLE USE POLICY
2017-18

Seton Catholic Schools is committed to student use of technology as a tool to expand learning opportunities and conduct scholarly research. The use of technology facilitates global collaboration -- a vital skill for our 21st Century learners. Netbooks and campus computers are strictly for educational use consistent with the educational goals of Seton. Along with the opportunity this provides comes responsibility. This Acceptable Use Policy provides clear and concise guidelines regarding the appropriate use of all Seton owned technology. The underlying premise of this policy is that all members of the Seton community must uphold the values of honesty and integrity. The proper use of technology reflects the strength of one's character, as does one's behavior. We expect our students to exercise good judgment and to utilize technology with integrity.

➢ **Student owned Electronic Devices**
Student owned electronic devices are not permitted to use our networks.
In addition, Student cell phones are to be powered off **8:00AM – 3:15PM Each school day.**
Creating hot spots, share points or other similar services are prohibited.

Chatting and Blogging
◆ Any type of instant messaging is prohibited on campus except as a part of an assigned, in-class activity that is supervised by faculty or administration.
◆ Blogging is to be utilized on campus for academic purposes only.
◆ Participation in chat rooms during school hours is prohibited during the school day, except as part of an assigned, in-class activity.

Audio and Video
◆ Audio on all computers should be turned off, unless it is required for a classroom activity.
◆ Listening to music with earphones is permitted on campus only with the permission of the teacher. The music should reside local on you device and NOT STREAMED from music streaming services.
◆ The use of netbooks to watch movies, DVDs, YouTube clips or videos, or any other type of video on any other platform, unless assigned by a teacher, is not permitted during the school day.
◆ When watching a video or listening to audio assigned by a teacher, earphones must be used.
◆ Any audio or video recording may be done only with the prior permission of all parties being recorded.
◆ Sharing of music, including iTunes music sharing, over the school network is strictly prohibited and is subject to appropriate consequences.

Games
◆ The viewing and/or playing of electronic games, online or otherwise, is not permitted during school hours except as part of an assigned, in-class activity.
◆ The school reserves the right to remove any games from a school-owned computer or prevent access to online games that are considered inappropriate (games that include

violence, adult content, inappropriate language, weapons, etc.) or impede the educational learning environment.

Netbooks
◆ All netbooks are the property of Seton Catholic Schools and are not a student's personal property.
◆ Netbooks must not be left unattended at any time.
◆ Netbooks must be in a student's possession, in a secured, locked classroom, or in the student's locker at all times. Any netbook that is found to be unattended will be turned in to the Administration and/or the Technology Department.
◆ A Student should not lend his/her netbook to any other student or borrow a netbook from any other student. If a student's netbook is unavailable for use due to repairs, the student should see the Technology Department for a loaner.
◆ Netbooks should be carried and transported in a case at all times.
◆ Students are entirely responsible for backing up their own data. Lost or damaged data is not the responsibility of the school.
◆ No food or beverages should be in the vicinity of the netbooks. Netbooks may not be used in the cafeteria during lunch.
◆ Netbooks should be handled with respect and care. Inappropriate treatment of school netbooks is not acceptable.
◆ School-issued netbooks should be kept clean and may not be written on, have stickers applied to them, or be defaced in any way. If any of the preceding conditions are violated, a cleaning fee of $15 will be assessed and the netbook will be restored to an acceptable condition.
◆ Students are not allowed to create or access any administrative accounts on school computers. Attempting to bypass security is a violation.
◆ Fully charged batteries in a netbook should last for up to 8 hours with proper care and battery management; therefore, all netbooks must be charged completely before arriving at school.
◆ In extraordinary circumstances, charging a netbook in a classroom may be permissible. It is up to the discretion of the individual teacher for this privilege and all permission must be obtained from that teacher before it is permitted.

Network Access
◆ Students must not make any attempt to access servers or network information that is not open to the public.
◆ The utilization of any service intended to bypass the content filter or administrative restrictions is strictly prohibited and is subject to disciplinary action.
◆ Students may not use the school network for personal or private business reasons.
◆ Students may not connect personal devices to the school WiFi network without administrative approval.
◆ Students are not to knowingly degrade or disrupt online services. This includes tampering with computer hardware or software, vandalizing data, invoking computer viruses, attempting to gain access to restricted or unauthorized network services, violating copyright laws, or using any program that will disrupt the network. Any student found to be degrading or disrupting online services is subject to disciplinary action.
◆ Seton is not responsible for damaged or lost data transferred through our network or stored on a student netbook, campus computer, or our file servers.

Printing

◆ Students may print from their netbooks to designated printers on the Seton network.
◆ Printing at home is permissible
◆ Unauthorized file sharing of any kind is prohibited both on and off campus.
◆ File sharing is only permitted when it is needed for a specific assignment given by a faculty member.
  ■ File-sharing is defined as the public or private sharing of computer data or space. Any program that creates a point–to–point connection between two or more computing devices for the purpose of sharing data is considered a file sharing program.
◆ There is a $15 re-imaging charge to remove any unapproved software or files.

Deleting Files

◆ Do not delete any folders or files that you did not create or that you do not recognize. Deletion of certain files will result in a computer failure and will interfere with your ability to complete class work and may affect your grades.
◆ There is a $15 re-imaging charge to correct system files.

Downloading and Loading of Software

◆ Students may only install approved applications at the direction of a teacher or the Technology Department. The installation of software from any other source without permission is strictly prohibited.
◆ The downloading of music files, video files, games, etc. through the school's network is absolutely prohibited unless it is part of an assigned, in-class activity.
◆ The school reserves the right to remove any unapproved software that has been loaded onto a computer.
◆ Copyrighted movies may not be ripped from DVDs or downloaded from any source and placed on the netbooks.
◆ Only commercial videos (such as television programs) legally purchased from the iTunes music store or another like entity may be downloaded to the netbooks.
◆ There is a $15 re-imaging charge to remove any unapproved software or files.

Screensavers and Wallpapers

◆ Inappropriate or copyrighted media may not be used as a screensaver or background wallpaper.
◆ The use of images, gifs, or videos that display weapons, pornographic materials, inappropriate language, alcohol, drugs, or gang related symbols and/or pictures will result in disciplinary action.
◆ There is a $15 re-imaging charge to remove any of the above.

Internet Use

◆ The Internet is a rich and valuable source of information for education. Inappropriate materials including, but not limited to, sexual or pornographic materials, extremist or militant materials, gambling, depictions of violence, and images that are intended to be abusive or harassing are strictly prohibited from being accessed or displayed.
◆ All information obtained through the Internet for use in an assignment must be properly cited and be in compliance with copyright laws.
◆ Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.

◆ Plagiarism includes the use of any information obtained from the Internet that is not properly cited. Plagiarism of Internet resources will be treated in the same manner as any other incidences of plagiarism.

◆ If a student accidentally accesses a website that contains obscene, pornographic or otherwise offensive material, he/she is to notify a teacher or a member of the Technology Department as quickly as possible so that such sites can be blocked from further access. This is not merely a request; it is a responsibility.

Privacy, Use, and Safety

◆ Unless a student is completely sure of the identity of the person with whom they are communicating, students may not provide any personally identifiable information regarding themselves or any other person including name, phone number, address, passwords, etc. Frequently the identity of someone on the Internet is impossible to confirm, therefore, contact with such individuals is considered inappropriate and unsafe.

◆ Students are not to provide any type of personally identifiable information for any student, faculty member, or administrative personal to anyone outside of the school without that person's express permission.

◆ All students will be issued a username and password to access their netbook and any other Seton educational accounts through the Technology Department. In order to protect the privacy of each student, it is important that all students safeguard this information. DO NOT share passwords or usernames. Students are not permitted to add additional accounts or create personal passwords on a netbook.

◆ Seton respects the privacy of every student, faculty member, and administrator with respect to stored files and e-mail accounts. However, if inappropriate use, including honor code violations, or harassment are suspected, the school administration has the right to view any files in order to investigate suspected inappropriate behavior.

◆ The school will monitor or log all activities that take place on school-issued computers including, but not limited to web access and application usage.

◆ Students are prohibited from accessing faculty, administration, and staff computers as well as school file servers for any reason without explicit permission from the user or administrator of that computer.

◆ Students are prohibited from utilizing the command prompt interface. In addition to this, students are prohibited from using any method to obtain control of another person's computer through the use of their own computer.

◆ Students are prohibited from utilizing any unauthorized method of file sharing between computers.

◆ Cyberbullying is the use of electronic information and communication devices to willfully harm either a person or persons through any electronic medium, such as text, audio, photos, or videos. Examples of this behavior include but are not limited to:
  - Sending/posting false, cruel, hurtful or vicious messages/comments
  - Creating or contributing to websites that have stories, cartoons, pictures, and jokes ridiculing others
  - Breaking into an email account or other social media account and sending vicious or embarrassing materials to others
  - Engaging someone in electronic communication, tricking that person into revealing sensitive personal information and forwarding that information to others
  - Posting a picture of a student, administrator, faculty member, or staff member without prior permission.

- Any electronic communication that creates a hostile, disruptive environment on the school campus is a violation of the students and staff member's right to be safe and secure. Actions deliberately threatening, harassing, and intimidating an individual or group of individuals; placing an individual in reasonable fear of harm; damaging an individual's property; or disrupting the orderly operation of the school will not be tolerated.
- Netbooks that are provided by the school continue to be the property of the school. Therefore, the school has the right to view all content at any time.
- Any electronic device used on the school network is subject to all policies and consequences of the Acceptable Use Policy including: the right to view the content of the device at any time; the right to remove content from the device; and the right to retain the device in the school's possession if there is an infraction to the AUP that merits this consequence.
- Unauthorized duplication, installation, alteration, or destruction of data programs, hardware, or software is prohibited.
- Data, programs, hardware, software, and other materials including those protected by copyright may not be transmitted or duplicated.
- No identifiable photographs of students, faculty, or administration will be allowed to be published on the Internet or used in print without appropriate written consent. Concerning a student, appropriate written consent means a signature by a parent or legal guardian of the student.

Consequences
- The school reserves the right to enforce appropriate consequences for the violation of any section of the Acceptable Use Policy. Such consequences could include the loss of privileges on a netbook, the loss of the use of the computer for an amount of time, time in the penalty mode determined by the administration and members of the Technology Department, possible disciplinary action, and possible legal action.
- Computers with illegal or inappropriate software or materials on them will be reformatted or "re-imaged," and the student will be charged a $15 re-imaging fee PER incident for this service. This amount may be increased for repeat violations.
- In the case of repeated netbook abuse and/or damages, the school has the right to revoke the use of the school's netbook and the student will be restricted to using only on-campus computers. Repeated AUP offenses or netbook abuses may lead to the loss of a student's privilege of using a netbook on campus.
- Students are to report any known violations of this Acceptable Use Policy to appropriate administrative staff members. Random checks of student netbooks will be conducted throughout the year to ensure that these policies are being followed.
- Seton takes no responsibility for activities conducted on school computers and netbooks or materials stored on computers, netbooks, or the school's network.

Social Media Policy

Saint Elizabeth Ann Seton Catholic Schools' social media policy is covered under a separate document and is available on our Web site at www.Setonschoools.org

ACCEPTABLE USE POLICIES FOR ONLINE SERVICES
Seton Catholic Schools - 2017-18

Students are required to adhere to all provisions and conditions set forth in this Acceptable Use Policy and Social Media policy. Any violations of this policy will result in disciplinary action, the loss of netbook privileges, and/or possible legal action.

Students are to report any known violations of this Acceptable Use Policy to appropriate staff members. Seton Catholic School takes no responsibility for activities conducted on school computers and netbooks or materials stored on computers, netbooks, or the network.

I agree to abide by the guidelines of the Acceptable Use Policy as described above and the Social Media policy posted on our website. . I understand that there will be consequences for not adhering to these guidelines. These consequences could include the loss of netbook privileges for serious infractions.

Grade _____

Student Name _____

Student's Signature _____   Date _____

Parent's Name _____

Parent's Signature _____   Date _____