ST. BENEDICT PARISH & PREPARATORY SCHOOL

ACCEPTABLE USE AGREEMENT FOR SBPPS NETWORK 2018-19

Purpose

The purpose of the St. Benedict Parish & Preparatory School (SBPPS) computer network is to advance and promote ministerial and educational opportunities, innovation and educational excellence, and to provide users access to a world wide array of ministerial and educational resources. Access to the resources of the network will improve learning and teaching through research, access to information, teacher training, collaboration and dissemination of successful educational practices, methods, and materials.

The Internet

The Internet is a vast, global network, linking computers with universities, schools, laboratories and other sites. Through the Internet, one can communicate with people all over the world through discussion forums and electronic mail. In addition, many educationally valuable files may be downloaded from the Internet. Due to its enormous size and resources, the Internet's educational potential is boundless. Via its broad reach, however, the Internet also contains the potential for abuse. SBPPS is not responsible for assuring the accuracy or usability of any information found on external networks. For safety purposes, SBPPS employs a firewall.

User Access

Internet access is provided through the SBPPS network system. All users will have access to the Internet. The use of the Internet and SBPPS network is a privilege, not a right, thus

all users must submit a signed Acceptable Use Agreement to gain access to the Internet and network.

Grades K-4: Students in Grades K-4 will gain access to the Internet after they take part in a discussion of this agreement with a parent or guardian. A parent or guardian is required to sign the Acceptable Use Agreement.

Grades 5-12: Students in Grades 5-12 will gain access to the Internet once the student and student's parent or guardian have submitted a signed Acceptable Use Agreement.

St. Benedict Preparatory School Staff, Volunteers and Guests may gain access to the Network/Internet once they have submitted a signed Acceptable Use Policy. - Signing the teacher/faculty handbook is the signature page for the AUP.

Users' Responsibility

Your right to free speech applies to communication on the Internet. The Internet is considered a limited forum, similar to the school newspaper, and therefore the SBPPS may restrict speech for valid educational reasons. The SBPPS will not restrict your speech on the basis of a disagreement with the opinions you are expressing. However, the school reserves the right to restrict speech if it undermines or directly opposes the value, beliefs and tenants of the Roman Catholic Faith.

All student use of the Internet will be conducted under faculty supervision. Nevertheless, faculty members are not expected to monitor student's use at every moment. Each student is expected to take individual responsibility for his or her appropriate use of the Internet.

Users are responsible for making back-up copies of the documents that are critical to their use.

Users are responsible for immediately notifying the computer teacher or principal of any possible security problems or of damage to the computer to which they are assigned**.**

The SBPPS assumes no responsibility for unauthorized charges, costs or illegal uses.

Internet Access

Inappropriate conduct on the SBPPS Internet will be subject to disciplinary action, in conformity with the St. Benedict Preparatory School rules on Student Conduct and Discipline (which is published in school handbooks). The administration may deny user access to the network. Further, any user identified as a security risk or having a history of problems with other computer systems may be denied access to the SBPPS network.

Privacy and Administrators' Access to User Files

Network storage areas (including user files) will be treated like school lockers may be subject to inspection. Internet (email) messages are public communication and are not private. All communications including text and images may be subject to applicable law enforcement or other third parties without prior consent of the sender or the receiver. Network administrators may review communications (email, attachments, files) to maintain integrity system-wide and ensure that users are using the system in a responsible manner. ALL users, regardless of position or relationship with SBPPS, should not assume that uses of the SBPPS network are private. All users are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

Personal Safety

The Internet is accessible to the public. Unfortunately, this includes people who want to make contact with students for inappropriate purposes or under false pretenses. Although SBPPS employs both a filter and firewall, screening the Internet for such inappropriate uses is still difficult. Therefore, users should never reveal their full name, address or telephone number, nor should they arrange a meeting with a person who was met on-line. Users should promptly inform the school administration of any on-line communication that is threatening, harassing, or otherwise inappropriate.

Network Etiquette

Users are expected to learn and to abide by generally accepted rules of Internet network etiquette, as well as rules of a Catholic parish and school decorum. These include common courtesy, politeness, professionalism, and the avoidance of vulgar language. Try

to avoid sarcasm and humor; without face-to-face communication, your **comments** may be misinterpreted or viewed as criticism. Don't publicly criticize or anger others. Use all capitals only to highlight a word; if you use them for an entire message, people will think you're shouting at them.

Unacceptable Uses of the St. Benedict Parish & Preparatory School Network

The following are unacceptable uses of the SBPPS network:

- The school uses a web proxy and content filter both on campus and on the cloud. **Any attempt to bypass these services in any fashion is strictly prohibited**.
- Sharing your password or other credentials with anyone.
- Posting private or personal information about another person.
- Reposting personal communication without authors prior consent.
- Using a school computer without knowledge/approval of school personnel responsible for the computer
- Changing or attempting to alter any configuration, program or password on any computer or system (approved school personnel may be permitted to change their own passwords at the discretion of the administration).
- Attempting to access system files, security files or another person's files.
- Accessing or transmitting unacceptable, obscene, pornographic, or illegal material.
- Posting chain letters or engaging in "spamming." ("Spamming" means sending annoying or unnecessary messages to large numbers of people.)
- Engaging in sexual harassment. The SBPPS Sexual Harassment Policy, which is included in the individual schools' handbooks, is applicable to Internet conduct.
- Engaging in bullying or harassment in any manner of anyone having a relationship with SBPPS. The SBPPS Anti-Bullying Policy, which is included in the individual schools' handbooks, is applicable to Internet conduct.
- Participating in any communications that facilitate the illegal sale or use of drugs or alcohol; that facilitate criminal gang activity; that threaten, intimidate, or harass any other person; that facilitate gambling. The system/network may not be used for illegal purposes, in support of illegal activities or for any activity prohibited by district policy.
- Communications. Users are responsible for the content of all text, audio or images that they place or send over the Internet. Fraudulent, harassing or obscene messages are prohibited. No abusive, profane or offensive language, pictures, or gestures of any kind should be used to communicate on the SBPPS or on the Internet.
- Plagiarism. "Plagiarism" means taking material created by others and presenting it as if it were one's own words.
- Infringing copyrights. One copy of copyrighted material may be downloaded for a user's personal use. Copyright infringement occurs when a person inappropriately reproduces or transmits material that is protected by copyright. For example, most

software is protected by copyright and may not be copied without the permission of the copyright owner and systems administrator.

- Inappropriate materials. Access of material that has been deemed inappropriate for educational or ministerial use is prohibited. Should users encounter such material by accident, they should disengage**.**
- Participating in **private or commercial** activities that are not directly related to educational purposes of the SBPPS.
- Violating student rights or employee rights to privacy/confidentiality, or unauthorized disclosure, use, and dissemination of personal identification information;
- Using the Internet for entertainment or limited-discovery function without permission;
- Downloading, installing or storing software on a school computer without the approval of appropriate school personnel;
- No user shall engage in communication that represents personal views as those of the SBPPS or that could be misinterpreted as such.

Behaviors And Consequences

Appropriate Codes of Conduct and Disciplinary Measures are outlined in the school handbook for students, and in the faculty handbook for faculty and staff. The school administration reserves the right to administer appropriate consequences for inappropriate technology use, access and behavior.

- Tampering with computer security systems and/or applications and/or documents and/or equipment will be considered vandalism, destruction, and defacement of school property. Please be advised, it is a federal offense (Felony) to break into any security systems. Financial and legal consequences of such actions are the responsibility of the user (staff, volunteer, student) and student's parent or guardian.
- Any student or employee to attempts to bypass the school security services will face disciplinary consequences.
- Any student or employee using another person's credentials to access applications or the network (whether or not the person knows/approves) will face disciplinary action. NEVER USE ANOTHER PERSON'S CREDENTIALS. Ever. Seek supervisor assistance if needed.
- Vandalism will result in cancellation of privileges, disciplinary action and restitution for costs associated with hardware, software, and system restoration. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, hardware, software or the network. This includes, but is not limited to, the uploading or creating of computer viruses.

- In the event that there is a claim that a **student user** has violated any of the Acceptable Use Agreement, she/he will be provided with written notice of the suspected violation and given an opportunity to be heard by the school administrator.
- In the event that there is a claim that **an employee user** has violated any of the Acceptable Use Agreement, she/he will be provided with written notice of the suspected violation and given an opportunity to be heard by the school administrator.

Notifications

Any student, teacher, staff member or volunteer must notify the systems administrator or assistant systems administrator if they have identified a possible security problem. Do not go looking for security problems, as this may be construed as an illegal attempt to gain access to inappropriate areas. Further, they should report encounters with inappropriate material to their school administrator immediately.

Changes in the St. Benedict Parish & Preparatory School Acceptable Use Agreement

St. Benedict Parish & Preparatory School reserves the right to change this agreement at any time. Statements in this Acceptable Use Policy are subject to amendment with or without notice. The school administration will attempt to keep school families informed of all changes as soon as practical. Some changes might be made immediately due to unforeseen circumstances.

Electronic Communications User Agreement

As an employee or student of St. Benedict Parish and Preparatory School, I have read the information about the appropriate use of the SBPPS Network and Internet Access. I understand this agreement and its' outline of the Use and Misuse of the Network, as well as the Limits of Privacy inherent in Electronic Communications via the Network.

- I agree to comply with the terms of this agreement.
- I agree to never allow another user to access the network with my ID or Password.
- I understand that failure to comply with the policies listed in this document can result in actions ranging from denial of future access to expulsion (termination of employment for employees).
- I further agree to review and comply with applicable acceptable usage guidelines.

Student Name _____ Student Grade _____

Student Signature _____

I have discussed this agreement with my child and will support SBPPS's enforcement of the Acceptable Use Policy.

Parent Signature _____ Date _____