To gain access to the Internet, all students must obtain parental permission as verified by the signatures on the attached form. Should a parent prefer that a student not have Internet access, use of the computers is still possible for more traditional purposes such as word processing, however it will mean that in some instances the student will need to be removed from the computer lab or class environment while instruction is going on.

The use of the school's internet connectivity resources and equipment is a privilege, not a right, and may be revoked if abused. The user is personally responsible for his/her actions in accessing and utilizing the school's computer resources. Students should never access, save, or send anything that they would not want their parents or teachers to see.

Definitions

Electronic communication includes, but is not limited to, the following: communications or depictions through email, text messages, direct messaging, private messaging, website postings, or social media whether they occur through the school's equipment, connectivity resources (e.g., WiFi) or using a personal device.

1. *Professional* **electronic communication** is a work-related activity that addresses instructional, educational, or extra-curricular program matters.
2. *Personal* **electronic communication** use is a non-work related activity.

Social media is defined as any form of online publication *.pr* presence that allows interactive communication, including, but not limited to social networks·, apps, blogs, internet websites, internet forums, and wikis. Examples of social media include, but are not limited -to, Facebook, Twitter, lnstagram, Snapchat, Vine, Whatsapp, YouTube, Google+, and Flickr. Additional social media may be developed in the future that could be covered by this policy.

ACCEPTABLE USAGE:

Students are responsible for appropriate behavior on the Internet just as they are in a classroom or on campus grounds. Communications on the Internet are often public in nature. General school rules for behavior and communications apply. It is expected that users will comply with school policy as referenced in the Parent/Student Handbook and the specific rules set forth below.

Whether the communication occurs within or outside of school property, during or after school hours, when a student's use of electronic communication jeopardizes the safe environment of the school or is contrary to Gospel values, the student can be subject to the full range of disciplinary consequences, including expulsion. Violations of the school's electronic communication policy will be addressed in conformance with the school's disciplinary policy as referenced in the Parent/Student Handbook.

The school reserves the right to confiscate and/or examine any electronic device in the student's possession while on campus including, but not limited to, cellular telephones, watches, tablets, gaming devices, cameras, school-issued devices or other electronic communication equipment of any type.

Limited Access- Students may access only those websites to which, according to school policy, they have been given permission. The school follows state and federal laws regarding the use of filters on school computers connected to the internet. Students may also access websites that have been specified by the teacher for a specific class activity. If any student wanders outside of the boundaries of the site specified by the teacher or by school policy, this will be considered a severe policy infraction and may result in disciplinary action. Consequences will include but are not limited to: parental notification and the immediate suspension of school's equipment or network privileges for a period of no less than two weeks. If the behavior is repeated, equipment or network privileges will be suspended for the rest of the school year.

Privacy - Users of the school's equipment or network should have no expectation of privacy in anything they create, store, send, receive or display on or over that equipment or using those connectivity resources, which includes personal files. Administrators and or teachers may review activity to maintain system integrity and ensure that employees and students are using the system responsibly.

Storage capacity- Employees and students are to store all materials as specified by the computer or classroom teacher.

Illegal copying - Students should never download or install any commercial software, shareware, or freeware onto a school computer unless they have written permission from the school's technology coordinator. Nor should any student copy other people's work or intrude into other people's files.

Prohibited electronic communication - The are following types of electronic communication are prohibited: (1) electronic communication of a sexual nature; (2) electronic communication with the intent to or does threaten, libel, slander, malign, disparage, harass or embarrass members of the school community; (3) any action that violates the school's existing behavioral standards covered by the Parent/Student Handbook; or (4) any action that causes harm to the school community, regardless of where the electronic communication occurs or originates from.

Electronic communication by or between students - The school provides opportunities for education on digital citizenship for students.

Electronic communication between teaching and school staff and students - Electronic communication between school staff and students must be professional and should only be used to address instructional, educational, and extra-curricular program matters. Personal electronic communication between teacher and student is prohibited until the student has graduated and is over 18 years of age.