This document must be signed and on file with the school before students will have technology (computer) privileges.

BISHOP GARCIA DIEGO HIGH SCHOOL
ACCEPTABLE USE POLICY FOR
COMPUTERS, NETWORK, INTERNET, AND ELECTRONIC COMMUNICATIONS

Bishop Garcia Diego High School ("BGDHS") information technology resources, including email and Internet access, are provided for educational purposes. Adherence to the following policy is necessary for continued access to the school's technological resources:

Students must
1. Respect and protect the privacy of others.
   o Use only assigned accounts.
   o Not view, use, or copy passwords, data, or networks to which they are not authorized.
   o Not distribute private information about others or themselves.
2. Respect and protect the integrity, availability, and security of all electronic resources.
   o Observe all network security practices, as posted.
   o Report security risks or violations to a teacher or the network administrator.
   o Conserve, protect, and share these resources with other students and Internet users.
   o Vandalism or hacking will result in termination of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, network, or agency that is connected to the Internet. This includes, but is not limited to, the uploading/downloading of any computer games and viruses, attempts at gaining unauthorized access, willful damage to computers and peripherals, or changing on-line materials without permission.
   o All students are provided with an Edline “file locker” to allow documents to be transported between home and school.
   o Flash drives are not permitted in any school computer without the consent of the teacher in charge or the network administrator.
3. Respect and protect the intellectual property of others.
   o Not infringe copyrights (no making illegal copies of music, games, or movies).
   o Not plagiarize.
4. Respect and practice the principles of community.
   o Communicate only in ways that are kind and respectful.
   o Report threatening or discomforting materials to a teacher.
   o Cyberbullying of any student or school employee is prohibited through the use of data or computer software that is accessed through a computer, computer system, or computer network of BGDHS, or off-campus if it causes emotional distress to an individual that substantially disrupts or interferes with the operation of the school or an individual student’s ability to receive an education. Cyberbullying includes, but is not limited to the following: posting slurs or rumors or other disparaging remarks about a student or school employee on a web site or on a web blog; sending e-mail or instant messages that are mean or threatening, or so numerous as to drive up
the victim’s cell phone bill; using a camera phone to take and send embarrassing photographs of students or school employees; posting misleading or fake photographs of students or school employees on web sites.

- Not intentionally access, transmit, copy, or create material that violates the school’s code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
- Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
- Not use the resources to further other acts that are criminal or violate the school’s code of conduct.
- Not send spam, chain letters, or other mass unsolicited mailings.
- Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.
- Gaming on campus is prohibited. Gaming uses excessive amount of bandwidth and slows the network for others.

**Consequences for Violation.**

Violations of these rules may result in disciplinary action, including the loss of a student’s privileges to use the school’s information technology resources. Specific details may be found in the Parent-Student Handbook.

**Supervision and Monitoring.**

School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that users are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school’s information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of a crime to law enforcement.

**I ACKNOWLEDGE AND UNDERSTAND MY OBLIGATIONS:**

________________________________________________________________________

Student Signature  __________________________

Date

________________________________________________________________________

Print Student Name

________________________________________________________________________

Student Signature  __________________________

Date

________________________________________________________________________

Print Student Name

________________________________________________________________________

Parent/Guardian Signature  __________________________

Date

Only one form is required per family, however, EACH student must sign.