6 – TECHNOLOGY & TELECOMMUNICATIONS

6.1 Technology Acceptable Use Policy Agreement (for Parents & Students)

Epiphany Catholic School (ECS) offers students access to technology resources for educational purposes, which may include computer hardware and software licensed to the school. To gain access to the technology resources, all students must obtain parental permission as verified by the signatures on the Permission for Internet Usage, Media Release. & Parent-Student Handbook Acknowledgement located on the last page of this handbook. Should a parent prefer that a student not have internet access, use of the computer is still possible for more traditional purposes such as word processing. However, all students without parental permission ill not be able to go to the computer lab nor participate in projects which require research. Research will have to be done outside of school hours.

6.2 Internet Access

Internet access will enable students to explore thousands of libraries, databases, museums, and other repositories of information and to exchange personal communication with other internet users around the world. Families should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive. While the purpose of the school technology and Internet access is for constructive purposes, students may find ways to access other materials. The school has a firewall that prevents students from entering inappropriate sties and is continuously updated. The school believes that the benefits to students from access to the Internet outweigh the disadvantages. However, ultimately the parents/guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Therefore, the school supports and respects each family's right to decide whether or not to all for access.

6.3 Expectations

Whether occurring within or outside of school, when a student's use of technology jeopardizes the safe environment of the school, staff or students, or is contrary to Gospel values, the student can be subject to the full range of disciplinary consequences including the expulsion of the student.

Students are responsible for appropriate behavior on the school's computer network just as they are in a classroom or anywhere on campus. Communications on the network are often public in nature. General school rules for behavior and communication apply. It is expected that users will comply with Archdiocesan standards and the specific rules set forth. The use of technology resources 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 technology resources. The students are expected to never access, keep, or send anything that they would not want their parents or teachers to see.

6.4 Rules of Appropriate Use

Electronic Communication – Students may not use electronic communication in a way that jeopardizes the safe environment of the school, staff, or students or is contrary to Gospel values.

This policy applies to all forms of electronic communications or depictions whether they occur through the school's equipment or connectivity resources or through private communication.

Personal Safety and Personal Privacy – Student will not post personal contact information about themselves or others unless otherwise indicated in the user agreement and parent permission form. Personal contact information includes their address, telephone, school address, etc. This information may not be provided to an individual, organization, or company, including websites that solicit personal information.

Social Networking – Accessing social networking websites and/or applications, except those used for educational purposes and as directed, are off-limits on school property. The use of circumventors to get around school network security is prohibited.

Illegal Copying – Students should never download or install any commercial software, shareware, or freeware onto network drives, external devices or cloud-based storage. Nor should students copy other individual's work or intrude into other individual's files. The download/upload of any material in violation of any U.S., State, Board, Archdiocesan, or school policy is prohibited. This includes, but is not limited to, copyrighted materials, threatening, violent, obscene material, or material protected by trade secret.

Inappropriate materials or language – No profane, abusive, slanderous, bullying, or impolite language or images should be used to communicate, nor should materials be accessed which are not in line with the rules of school behavior. Use of technology resources for anything other than educational purposes is also prohibited. Should students encounter inappropriate materials by accident, they should report it to their teacher immediately. A good rule to follow is never view, send, distribute, or access materials or images, which you would not want your teachers and parents to see. Use of any electronic device to transmit unacceptable language, images, and/or photos that are harmful to self or others is prohibited.

Succinct Advice

These are guidelines to follow to prevent the loss of technology privileges and/or disciplinary measures at the school.

1. Do not use technology to harm self, other people, or their work.
2. Do not damage the network any technology resources in any way.
3. Do not interfere with the network or computer operation by installing any form of software or permitting the spread of computer viruses.
4. Do not violate any copyright laws.
5. Do not view, send, distribute, or display offensive or bullying messages or images.
6. Do not share your passwords/personal information of in any way obtain another persons' password/personal information.
7. Do not waste technology resources such as storage space or printing supplies.
8. Do not trespass in another's folders, work, or files.
9. Notify an adult immediately, if by accident, you encounter materials, which violate the Rules of Appropriate Use.
10. Do not attempt to circumvent network filters or security in any way.

11. Be prepared to be held accountable for your actions and for the loss of privileges if the Rules of Appropriate Use are violated.