DIOCESE OF TRENTON
ACCEPTABLE USE OF TECHNOLOGY POLICY

PURPOSE

This policy provides the procedures, rules, guidelines and codes of conduct for the use of technology. Use of such technology is a necessary element of the mission of Catholic schools, and is provided to users as a privilege, not a right. Schools seek to protect, encourage, and enhance the legitimate uses of technology by placing fair limitations on such use and sanctions for those who abuse the privilege.

SUMMARY

Technology that includes but is not limited to computers, wireless & LAN access, electronic mail, Internet access, and all other forms of instructional, networking and communication tools are provided as a service by the school to users.

Use of these technologies is a privilege, not a right. Users are required to be good technology citizens by refraining from activities that disrupt education, or can be considered as illegal, immoral, and/or unprofessional conduct.

The user is responsible for his/her actions in accessing technology. Failure to comply with the guidelines of technology use may result in the loss of privileges and/or appropriate disciplinary action. Severe violations may result in civil or criminal action under the New Jersey Statutes or Federal Law.

PARENTAL RESPONSIBILITY

Given the dynamic nature of technological advancements and the volatile nature of resources available on the Internet, the school acknowledges its inability to completely regulate and monitor the information received or sent by users, although appropriate filters are used. As such, the school cannot assure parents or that users will be denied access to all inappropriate materials or sending or receiving communications contrary to the school's philosophy, goals, and educational mission.

In the case of students, parents or guardians should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. In addition, it is possible to purchase certain goods and services via the Internet that could result in unwanted financial obligations for which a student's parent or guardian would be held responsible.

GUIDELINES

1. Access to computers, networks and devices within the school network is a privilege and must be treated as such by all users.

2. The network will be used solely for the purpose of research, education, and school related business and operations.

3. Computer systems shall only be used by the authorized user's user account. Account owners are ultimately responsible for all activity under their account and shall abide by this policy. All communications must be in line with Catholic teaching.

4. All communications and information accessible and accessed via the school system is and shall remain property of the school.

5. Student use shall be supervised and monitored by authorized staff. Student use must be related to the school curriculum.

6. Staff use must be related to school business.

7. Any defects or knowledge of suspected abuse of the school systems, networks, security, hardware, or software shall be reported to the Technology Director.

UNACCEPTABLE USE

The school has the right to take disciplinary action, remove computer privileges, or take legal action for any activity characterized as unethical, unacceptable, or unlawful.

<u>Unacceptable use activities constitute, but are not limited to, any activity through which any user:</u>

1. violates this agreement, copyright, license agreements or other contracts.

2. interferes with or disrupts other users, services, or equipment. Disruptions include, but are not limited to, distribution of advertising and propagation of computer viruses or worms.

3. attempts to disable, bypass or otherwise circumvent the school's content filter that has been installed in accordance with the federal Children's Internet Protection Act. This includes but is not limited to the use of proxy servers and cellular hotspots.

4. seeks to gain or gains unauthorized access to information resources, obtains copies of, or modifies files or other data, or gains and communicates passwords belonging to other users.

5. uses or knowingly allows another to use any computer, network, system, program, or software to devise or execute a scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations.

6. destroys, alters, dismantles, disfigures, prevents rightful access to, or otherwise interferes with the integrity of computer-based information resources, whether on stand-alone or networked computers.

7. invades the privacy of individuals or entities.

8. uses the network for commercial or political activity or personal or private gain.

9. installs unauthorized software or material for use on School computers. This includes, but is not limited to, downloading music, pictures, images, games, and videos from either the Internet or via portable drives.

10. uses the network to access inappropriate materials.

11. uses a system to compromise its integrity (hacking software) or accesses, modifies, obtains copies of or alters restricted or confidential records or files.

12. submits, publishes, or displays any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.

13. uses the systems for illegal, harassing, vandalizing, inappropriate, or obscene purposes, or in support of such activities is prohibited. Illegal activities are defined as a violation of local, state, and/or federal laws. Cyber-bullying and harassment are slurs, comments, jokes, innuendos, unwelcome comments, cartoons, pranks, and/or other verbal conduct relating to an individual which:

    a) has the purpose or effect of unreasonably interfering with an individual's work.

    b) interferes with school operations.

    c) has the purpose or effect to cause undue emotional stress or fear in an individual.

THE SCHOOL'S RIGHTS AND RESPONSIBILITIES

1. Monitor all activity on the school's systems.

2. Determine whether specific uses of the network are consistent with this

Acceptable Use Policy.

3. Remove a user's access to the network at any time it is determined that the user is engaged in unauthorized activity or violating the Acceptable Use Policy.

4. Respect the privacy of individual user electronic data. The school will secure the consent of users before accessing their data, unless required to do so by law, policies of the diocese or policies of the school.

5. Take prudent steps to develop, implement, and maintain security procedures to ensure the integrity of individual and school data.

6. Attempt to provide error-free and dependable access to technology resources associated with the school system. The school cannot be held liable for any information that may be lost, damaged, or unavailable due to technical or other difficulties.

7. Ensure that all computer technology users complete and sign an agreement to abide by the school's acceptable use policy.

VIOLATIONS/CONSEQUENCES

Users who violate this policy will be subject to revocation of system access up to and including permanent loss of privileges, and discipline up to and including expulsion or termination of employment. Violations of law will be reported to the Superintendent of Schools of the Diocese of Trenton and law enforcement officials.

<u>Unacceptable use of the computer systems include, but are not limited to:</u>

1. altering any computer configuration.

2. installing or downloading any executable files from the Internet or portable drives.

3. using chat rooms or social web sites except for teacher-directed educational purposes.

4. Installing or using instant messenger programs.

5. downloading music or video files.

6. streaming online radio stations, movies and television programs.

7. writing, downloading, or printing files or messages that contain inappropriate language.

8. accessing or transmitting pornographic or other inappropriate material.

9. violating the rights to privacy of students and employees of the school.

10. reposting personal communications without the author's prior consent.

11. attempting to hack, crack, or otherwise degrade or breach the security of the school's network infrastructure, network devices, or individual computers.

12. attempting to bypass the school's content filter, including the use of proxy servers and hotspots.

13. developing or passing on programs that damage a computer system or network, such as viruses.

14. plagiarism.

15. modifying or copying files of other users without their consent.

16. giving out personal information such as address and phone numbers without staff permission.

17. accessing or transmitting material which promotes violence or advocates the destruction of property including information concerning the manufacture of destructive devices (explosives, bombs, fireworks, incendiary devices, etc.)

18. accessing or transmitting material which advocates or promotes violence or hatred against particular individuals or groups of individuals or is contrary to Catholic teaching.

19. accessing or transmitting material which advocates the use, purchase, or sale of illegal goods or services.

20. conducting or participating in any illegal activity.

21. performing any act that is determined as Cyber-bullying, harassment, or a violation of good Digital Citizenship.

22. any inappropriate use as determined by the president, director of technology and/or school administrators.