

Network/Internet Acceptable Use Policy

Technology Usage

Saint Patrick's School technology exists for the purpose of maximizing the educational opportunities and achievement of school students. Research shows that students who have access to technology improve achievement. In addition, technology assists with the professional enrichment of the staff and Board and increases engagement of students' families and other patrons of the school, all of which positively impact student achievement. The school will periodically conduct a technology census to ensure that instructional resources and equipment that support and extend the curriculum are readily available to teachers and students.

The purpose of this policy is to facilitate access to school technology and to create a safe environment in which to use that technology.

Definitions

For the purposes of this policy and related procedures and forms, the following terms are defined:

Technology Resources – Technologies, devices and resources used to access, process, store or communicate information. This definition includes, but is not limited to: computers, modems, printers, scanners, fax machines and transmissions, telephonic equipment, audio-visual equipment, Internet, electronic mail, electronic communications devices and services, multi-media resources, hardware and software.

User – Any person who is permitted by the school to utilize any portion of the school's technology resources including, but not limited to, students, employees, School Board members and agents of the parish.

User Identification (ID) – Any identifier that would allow a user access to the school's technology resources or to any program including, but not limited to, e-mail and Internet access.

Password – A unique word, phrase or combination of alphabetic, numeric and nonalphanumeric characters used to authenticate a user ID as belonging to a user.

Authorized Users

The school's technology resources may be used by authorized students, employees, School Board members and other persons such as consultants, legal counsel and independent contractors. All users must agree to follow the school's policies and procedures. Unless authorized by the principal or designee, all users must have a signed *User Agreement* on file with the school before they are allowed access to school technology resources. Use of the school's technology resources is a privilege, not a right. No potential user will be given an ID, password or other access to school technology if he or she is considered a security risk by the principal or designee.

User Privacy

A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the school's technology resources, including e-mail and access to the Internet or network drives. By using the school's network and technology resources, all users are consenting to having their electronic communications and all other use monitored by the school. A user ID with e-mail access will only be provided to authorized users on condition that the user consents to interception of or access to all communications accessed, sent, received or stored using school technology.

Electronic communications, downloaded material and all data stored on the school's technology resources, including files deleted from a user's account, may be intercepted, accessed or searched by school administrators or designees at any time in the regular course of business to protect users and school equipment. Any such search, access or interception will be reasonable in inception and scope and shall comply with all applicable laws.

Technology Administration

The Principal directs the staff to create procedures governing technology usage and to assign trained personnel to maintain the school's technology in a manner that will protect the school from liability and will protect confidential student and employee information retained on or accessible through school technology resources.

Administrators of computer resources may suspend access to and/or availability of the school's technology resources to diagnose and investigate network problems or potential violations of the law or school policies and procedures. All school technology resources are considered school property. Technology Administrators may maintain or improve technology resources at any time. Technology Administrators may remove, change or exchange hardware or other technology between buildings, classrooms or users at any time without prior notice. Technology Administrators may install or remove new programs or information, install new equipment, upgrade any system or enter any system to correct problems at any time.

Content Filtering and Monitoring

The school will monitor the on-line activities of minors and operate a technology protection measure ("filtering/blocking device") on the network and/or all computers with Internet access, as required by law. The filtering/blocking device will be used to protect against access to visual depictions that are obscene or harmful to minors, as required by law. Filtering/Blocking devices are not foolproof, and the school cannot guarantee that users will never be able to access offensive materials using school equipment. Evasion or disabling, or attempting to evade or disable, a filtering/blocking device installed by the school is prohibited.

The principal, designee or the school's technology administrator may disable the School's filtering/blocking device to enable a non-student user access for bona fide research or for other lawful purposes.

Closed Forum

The school's technology resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law. The school's webpage will provide information about the school, but will not be used as an open forum.

All expressive activities involving school technology resources that students, parents/guardians and members of the public might reasonably perceive to bear the imprimatur of the school and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the school for legitimate pedagogical reasons. All other expressive activities involving the school's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and school policies.

School Technology Prohibitions and Requirements

All Saint Patrick School network users are prohibited from:

1. Applying for a user ID under false pretenses or using another person's ID or password is prohibited.
2. Sharing user IDs or passwords with others is prohibited and users will be responsible for using the ID or password. A user will not be responsible for theft of passwords and IDs, but may be responsible if the theft was the result of user negligence.
3. Deleting, examining, copying or modifying files or data belonging to other users without their prior consent is prohibited.
4. Mass consumption of technology resources that inhibits use by others is prohibited.
5. Use of school's technology, including the telephone system, for soliciting, advertising, fundraising, commercial purposes or for financial gain is prohibited, unless authorized by the school.
6. Accessing fee services without permission from an administrator is prohibited. A user who accesses such services without permission is solely responsible for all charges incurred.
7. Users are required to obey all laws, including criminal, copyright, privacy, defamation and obscenity laws. The school will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using school technology in violation of any law.
8. The school prohibits the use of school technology resources to access, view or disseminate information that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, pervasively indecent or vulgar, or unlawful.
9. Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of school staff for curriculum-related purposes.

10. The school prohibits the use of school technology resources to access, view or disseminate information that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g., threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, they will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful school policies and procedures.

11. The school prohibits any use that violates any person's rights under applicable laws, and specifically prohibits any use that has the purpose or effect of discriminating or harassing any person on the basis of race, color, religion, sex, national origin, ancestry, disability, age, pregnancy or use of leave protected by the Family and Medical Leave Act.

12. The school prohibits any unauthorized intentional or negligent action that damages or disrupts technology, alters its normal performance or causes it to malfunction. The school will hold users responsible for such damage and will seek both criminal and civil remedies, as necessary.

13. Users may only install and use properly licensed software, audio or video media purchased by the school or approved for use by the school. All users will adhere to the limitations of the school's technology licenses. Copying for home use is prohibited unless permitted by the school's license and approved by the school.

14. At no time will school technology or software be removed from the school premises, unless authorized by the principal or technology administrator.

Technology Security and Unauthorized Access

All users shall immediately report any security problems or misuse of the school's technology resources to a teacher or administrator.

No person will be given access to school technology if he or she is considered a security risk by the principal or designee.

1. Use of school technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.

2. Use of school technology to connect to other non school systems, or non school networks is prohibited while on school grounds.

3. The unauthorized copying of system files is prohibited.

4. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any school technology are prohibited.

5. Any attempts to secure a higher level of privilege on the technology resources without authorization are prohibited.

6. The introduction of computer viruses, hacking tools or other disruptive or destructive programs into a school computer, network or any external network is prohibited.

Online Safety—Disclosure, Use, and Dissemination of Personal Information

1. All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet.
2. Student users are prohibited from sharing personal information about themselves or others over the Internet while at school or on school grounds.
3. A student user shall promptly disclose to his or her teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable.
4. Students shall receive or transmit communications using only school-approved and school managed communication systems. For example, students may not use web based e-mail, messaging, videoconferencing or chat services.
5. Employees shall not transmit confidential student information using school technology, unless designated for that use. Employees will take precautions to prevent negligent disclosure of student information or student records and will abide by all laws pertaining to student confidentiality.
6. No curricular or noncurricular publication distributed using school technology will include the address, phone number or e-mail address of any student without permission.

Electronic Mail

A user is responsible for all e-mail originating from the user's e-mail account.

1. Forgery or attempted forgery of e-mail messages is illegal and is prohibited.
2. Unauthorized attempts to read, delete, copy or modify e-mail of other users are prohibited.
3. All users must adhere to the same standards for communicating electronically that are expected in the classroom and that are consistent with school's policies and procedures.

Exceptions

Exceptions to school rules will be made for school employees or agents conducting an investigation of a use that potentially violates the law, school policies or procedures. Exceptions will also be made for technology administrators who need access to school technology resources to maintain the school's resources or examine and delete data stored on school computers as allowed by the school's retention policy.

Waiver

Any user who believes he or she has a legitimate educational purpose for using the school's technology in a manner that may violate any of the school's policies or procedures may request a waiver from the principal, or a designee.

Understanding

This policy must be signed by all school technology users or users parent or guardian before being allowed access to school technology.

Print Users Name

Sign Users Name

Print Users Guardian (If Needed)

(Sign Users Guardian (If Needed)

Date