TECHNOLOGY ACCEPTABLE USE POLICY 2023-24

St. Agnes School recognizes the various ways, both positive and negative, that students, teachers, and parents can use technology both in school and at home. Students, teachers and parents in our school should always strive to use technology in a responsible and ethical way as they work toward becoming or modeling responsible citizens of our global community.

As a community of faith that embraces technology, we recognize the following:

- Words transmitted using the Internet and related technologies are published materials, available for worldwide access, and are public documents.
- The values of dignity and respect for every person apply to all of our interactions with each other, be they in person or by virtual means.
- Using technology to publish opinions which are obscene, work against the values of dignity and respect of each person, or bring harm to the individual as well as to our school community are contrary to the mission of St. Agnes School.

St. Agnes School discourages students, teachers, and parents from using technology in irresponsible ways both at school and at home and will hold students responsible for their published words. Students, teachers, and parents who use technology in ways that are contrary to our mission will face disciplinary action, up to and including expulsion.

St. Agnes School is pleased to offer to the staff and students access to a computer network, electronic mail and the Internet for educational purposes. To gain access to the school's computer network, e-mail and the Internet, all students under the age of 18 must obtain parental permission and must sign and return this form to the Technology Coordinator. All staff members must sign this form and return it to the principal or Technology Coordinator.

Resource sharing and communication for both students and teachers have increased with access to telecommunications and to the Internet. It is imperative that members of the school community conduct themselves in a responsible manner consistent with federal and state law while utilizing the school's computers and network, in keeping with our philosophy of Catholic education. Access to the school's network, Diocesan e-mail and the Internet will enable students and staff members to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.

What are "Computer Resources?"
When used in this policy, the term "computer resources" refers to the school's entire computer network. This includes the school's computer system, file servers, application servers, communication servers, mail servers, fax servers, web servers, work stations, stand-alone computers, laptops, software, data files, and all internal and external computer and communications networks that may be accessed directly or indirectly from the school's computer network.

Who is a "User?"
When used in this policy, the word "users" refers to all students, employees, consultants, temporary workers, parents and other persons or entities who use or come into contact with the school's computer resources.

Ownership of the Computer Resources
The computer resources are the property of the school. Access to the computer resources is provided solely for the purpose of carrying out the educational and operational needs. All use of the computer resources must be supportive of the educational objectives and must be consistent with academic expectations. Use of computer resources is a privilege that may be revoked at any time.

No Expectation of Privacy
Users should never consider electronic communication to be either private or secure. E-mail can be stored indefinitely on any number of computers. Copies of your messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to non-existent or incorrect user names may be delivered to persons that you never intended.

St. Agnes School has the right, but not the duty, to monitor any and all aspects of its computer system. Users consent to allowing the school to assess and review all materials users create, store, or received on the computer system, Internet or any other component of the computer network. Users understand that the school may use human or automated means to monitor use of the computer resources. Such monitoring may include, but is not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and news groups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail sent and received by users. Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that users have an expectation of privacy in such access or materials. The school has global passwords that permit it to access all material stored on the computer system, regardless of whether that material has been encoded with a particular user's password.

Netiquette
Because we believe that dignity and respect for every person should apply to all of our interactions, users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

- Be polite. User messages should not be abusive to others.
- Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
- Do not reveal user personal address or phone number or the addresses and/or phone numbers of students or colleagues.
- Illegal activities are strictly forbidden.
- Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
- Do not use the network in such a way that you would disrupt the use of the network by other users.
- All communications and information accessible via the network should be assumed to be private property.

Quality of Communications
Users should make each electronic communication truthful and accurate. Users should use the same care in drafting e-mail and other electronic documents as you would for any other written communication. Please keep in mind that anything created or stored in the computer system may, and likely will be reviewed by others. Information published or otherwise distributed electronically is subject to the same policies and procedures regarding the distribution of school system information, including, but not limited to, policies regarding public requests for information and distribution of information to the public.

Security
Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be printed, stored on-line, or given to others. Users are responsible for all transactions made using their passwords. No user may access the computer system with another user's password or account. Users may not use the computer system to "snoop" or pry into the affairs of other users by unnecessarily reviewing their files and e-mail. A user's ability to connect to another computer system does not imply a right to connect to those systems unless authorized to do so. Each user is

responsible for ensuring that use of outside computers and networks, such as the Internet, does not comprise the security of the school's computer resources. This duty includes taking reasonable precautions to prevent intruders from accessing the school's network without authorization. Viruses can cause substantial damage to computer systems. Each user is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the school's network. All material not belonging to the school must be scanned for viruses by the technology staff prior to being placed on the school's computer system. Users should understand that their home computers and laptops might contain viruses. All disks, CDs, and flash drives transferred from these computers to the school's network must be scanned for viruses.

Offensive Material

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that some of these pages may include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocent search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk. Although the school provides filtering software to protect students to the highest degree possible, the school cannot guarantee that this material might come from a search and is not responsible for material viewed or downloaded by users from the Internet.

Prohibited Activities

Users may not send material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate. It does not matter how such material is sent, whether it is by e-mail or other form of electronic communication, such as bulletin board systems, news groups, or chat groups. Further, such material may not be displayed on or stored in the school's computers. Users encountering or receiving such material should immediately report the incident to the administration. Users must not alter the "from" line or other attribution-of origin information in e-mail, messages, or postings. Anonymous electronic communications are forbidden. Users must identify themselves honestly and accurately when participating in chat groups, making postings to news groups, sending e-mail, or otherwise communication on-line. Without prior written authorization from the administration, users may not do any of the following to the school's computers or networks:

- Copy software from their home computers;
- Provide copies of software to any independent contractors or clients of the school or to a third person;
- Install software on any of the school's work stations or servers;
- Download any software from the Internet or other on-line service to any of the school's work stations or servers;
- Modify, revise, transform, recast, adapt any software; or reverse engineer, disassemble or decompile any software.

Users who become aware of any such misuse of software or violation of copyright law should immediately report the incident to the administration. Unless expressly authorized by the administration, sending, transmitting, or otherwise disseminating propriety data or other confidential information is strictly prohibited. Users may not send unsolicited email to persons with whom they do not have a prior relationship with the express permission of the administration.

Users who take home school computers may use them for educational purposes only. Users may not use school computers for gaming, social networking, personal work, commerce, etc.

Social Networking

Social networking sites including but not limited to MySpace®, Facebook®, and Xanga® are very popular today. Users of these sites have little control over the content that "friends" post on their sites because these sites are in the public domain. With this in mind, no user shall create or maintain a public

electronic presence that in any way links to or publicizes St. Agnes School. The following guidelines apply:

- Users may not use school information such as logos, official seals, or photographs.
- Users may not link their personal website to the school's website.
- Users may not post inappropriate photographs or content (including information about the school, students, staff, or parents) containing any form of school identification from the school.
- Users may not post content, including blogs or online journals, linking them in any way to the school.
- Users may not post content, or engage in any topics that are not in keeping with the mission of the school
- Be mindful that on-line content is not private and there could be long-term ramifications.
- Faculty and staff should not friend parents or children unless given approval by the school principal

Cyber-bullying

Cyber-bullying is being cruel to others through electronic means by sending or posting harmful material using the Internet or other electronic means. This can be done through email, instant messaging, chat rooms, or online sites such as MySpace or Facebook.

St. Agnes School will not tolerate harassment in any form whether conducted on or off campus. Harassment will be handled as outlined in the school discipline policy. Parents or students who feel that they have been the victims of cyber-bullying should print a copy of the material and report the incident to the administration. Harassment reports will be investigated fully. Consequences may include, but are not limited to, the loss of computer privileges, detention, suspension, or expulsion from school. Users must:

1. Respect and protect the privacy of others.
    - Use only assigned accounts.
    - Not view, use, or copy passwords, data, or networks to which they are not authorized.
    - Not share passwords nor use another user's passwords.
    - Not distribute private or personal information about others or themselves.
2. Respect and protect the integrity, availability, and security of all electronic resources.
    - Observe all network security practices, as posted.
    - Report security risks or violations to a teacher or network administrator.
    - Not destroy or damage data, networks, or other resources.
    - Conserve, protect, and share network, hard drive, and printing resources with other network users
3. Respect and protect the intellectual property of others.
    - Not infringe upon copyrights (no making illegal copies of text, pictures, music, games, or movies).
    - Not plagiarize. Copying another's work, without giving credit to the source, will be considered cheating and subject to the plagiarizing policy in this handbook.
4. Respect and practice the principles of community.
    - Communicate only in ways that are kind and respectful.
    - Report threatening or inappropriate sites or materials to a teacher.
    - Not intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are inappropriate, 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.

Students are to notify an adult immediately, if by accident, he/she encounters material that violates the rules stated above.

System Abuse

- Using a computer account that one is not authorized to use.
- Obtaining a password for a computer account that one is not authorized to have.
- Using the school network to gain unauthorized access to any computer systems.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses and worms.
- Knowingly or carelessly allowing someone else to use your account who engages in any misuse or violation of acceptable use.
- Forging email messages.
- Attempting to circumvent data-protection schemes or uncover or exploit security loopholes.
- Masking the identity of an account or machine.
- Deliberately wasting computing resources.
- Downloading, displaying uploading or transmitting obscenity or pornography, as legally defined.
- Electronic communications, or changing, or deleting another user's files or software without the explicit agreement of the owner, or any activity which is illegal under California computer crime laws.
- Personal use which is excessive or interferes with the user's or others' performance of job duties, or otherwise burdens the intended use of the school network.

Copyright

In their use of computer resources, users must comply with all software licenses; copyrights; and all other state, federal, and international laws governing intellectual property and on-line activities. The ability to read, alter, or copy a file belonging to another user does not imply permission to read, alter, or copy that file. Users may not alter or copy a file belonging to another user without first obtaining permission from the owner of the file.

Internet and E-Mail Rules

All users are responsible for good behavior on school computer networks just as they are in a classroom or on school property. Communications on the network are often public in nature. General school rules regarding appropriate behavior and communications always apply when working with the school's computers and network. The network is provided to conduct research and communicate with others for educational purposes. Access to network services is given to all users who agree to act in a considerate and responsible manner. Parent permission is required for students under 18 years of age. Access is a privilege - not a right. Access entails responsibility. No student will be allowed on the network without signed consent. All users need to read and sign the Acceptable Use Policy at the beginning of each school year. Individual users of the school's computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with Diocesan standards and will honor the agreements they have signed. Network storage areas, like school lockers and classrooms, are the property of the school. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on school servers will always be private. All information is subject to the Freedom of Information Act and should not be deemed private. With this educational opportunity comes responsibility. The school will take steps, such as using filtering programs (software designed to restrict access), access controls, and monitoring by teachers, to restrict access to controversial material.

On a global information network, such as the Internet, however, it is impossible to restrict access to all potential inappropriate materials. It is the responsibility of all users to understand and abide by the Acceptable Use Policy to ensure that access to those resources provided by the school are not abused. The following actions are not permitted:

- Sending or displaying offensive, sexually explicit, pornographic messages or pictures
- Using obscene, sexually explicit, threatening language

- Harassing insulting or attacking others
- Revealing personal information i.e. address, school, phone number
- Damaging or vandalizing computers, computer systems or computer networks
- Violating copyright laws or use property of another individual or organization without permission
- Plagiarism
- Establishing any official representation of the school or Diocese without obtaining prior approval of school administration
- Using another's password
- Trespassing in another's folders, information, work or files
- Intentionally wasting limited resources i.e. inappropriate downloads, spamming, chain letters, etc.
- Using chat rooms without expressed permission of a faculty member
- Employing the network for commercial purposes
- Friending a student (if you are a teacher) or teacher (if you are a student) on a Facebook®, MySpace® or a social network site
- Blogging for non-educational purposes during school hours

Violations may result in a loss of access as well as other disciplinary or legal action.

TECHNOLOGY ACCEPTABLE USE AGREEMENT

User Agreement and Parent Permission

STUDENT AND PARENT AGREEMENT

Part 1. Before signing this form, please read and review all of the information above. Return this page with both the student's signature and parent/guardian signature(s) to the school office. Keep the St. Agnes School Technology Acceptable Use Policy for your reference when you are utilizing the available technology resources of St. Agnes School.

Part 2. I have read and agree to comply with the terms of this policy governing the use of the school's computer resources. I understand that a violation of this policy may result in a loss of access as well as other disciplinary or legal action. As a user of the computer network, I hereby agree to comply with the stated rules - communicating over the network in a responsible fashion while honoring all relevant laws, policies, regulations, and restrictions.

Parent name: _____

Parent signature: _____ Date: _____

Student name: _____ Grade: _____

Student signature: _____ Date: _____

PARENT PERMISSION

Part 3. As the parent or legal guardian of the minor student signing above, I grant permission for my son or daughter to access networked computer services such as electronic mail and the Internet. I understand that individuals and families may be held liable for violations. I also understand that the Acceptable Use Policy applies if I am a user of school technology.

Parent name: _____

Parent signature: _____ Date _____

PRIVACY

☐ Check here if you do not want to have pictures of you or your child posted on the school's website, on the school's social media pages, or in other school publications (ie. yearbook). For safety and privacy, student names are not posted with pictures used on the school's website.