ST. FRANCIS XAVIER Catholic School System

101 E Northland Avenue
Appleton, WI 54911
MAIN 920.735.9380
FAX 920.735.1787

ACCEPTABLE USE POLICY (AUP) FOR TECHNOLOGY

PURPOSE

Technology is a valuable and real-world educational tool. Our system is committed to teach its students, faculty, administrators, staff, and school community to work and to learn effectively with technology and to ensure responsible use of technology. The policy outlined below applies to all technology use including but not limited to internet use. This policy applies to all students, faculty, administrators, staff, volunteers, or community members allowed access to school technology resources. In some cases outside or personal uses of technology may be applicable under this policy.

SCOPE OF USE

The St. Francis Xavier School System recognizes that the digital world allows anytime, anywhere access. Uses mentioned in this policy apply to inside school use and may in certain instances apply to personal technology use and/or uses outside of school. Where personal outside use of technology threatens a likelihood of substantial disruption in school, including harming or interfering with the rights of other students or teachers to participate fully in school or co-curricular activities, these activities may be viewed as a violation of the Acceptable Use Policy and may be subject to disciplinary measures.

The types of electronic and digital communications referenced in this AUP include, but are not limited to, social networking sites, cell phones, digital cameras, text messaging, e-mail, voice over IP, chat rooms, and instant messaging.

GOAL

The system's goal to prepare its members for life in a digital global community. To this end, the system will:

- Integrate technology with curriculum to enhance teaching and learning
- Encourage critical thinking, communication, collaboration, and problem-solving skills
- Facilitate evaluation and synthesis of information
- Require ethical practices and provide education for internet safety and digital citizenship
- Provide a variety of technology-based tools and related technology skills

GENERAL GUIDELINES FOR EMPLOYEES AND OTHER ADULTS

1. System employees and those in volunteer positions should not communicate with current students using personal accounts of social media (e.g. Facebook, e-mail, Twitter, texting). If social media is used to communicate with current students it should be done with a professional account that uses school technology, has privacy settings that are open to all students, parents and administrators and has an educational purpose.
2. A teacher or adult must keep the language in posts and other electronic communication formal and always think before sending or posting. This should involve re-reading the language to make sure it cannot be mistake for being suggestive or inappropriate. An effective technique to maintain professionalism between students and teachers is to confine topics conveyed via electronic communication to school activities, class topics, or information that may clarify an assignment.
3. An employee should exercise care in setting appropriate boundaries, understanding that what is private in the digital world often has the possibility of becoming public, even without knowledge or consent.
4. Adults should never use electronic communication to gossip or discuss personal or personnel issues, especially with young people.
5. An employee should not make statements that would violate any of the system's policies, including its policies concerning discrimination or harassment or statements that are counter to Catholic teachings.
6. An employee must uphold the system's value of respect for the individual and avoid making defamatory statements about the system, school, its employees, its students, or their families.
7. An employee may not disclose any confidential information of the system or school, about any colleagues, or students and/or their families.
8. An employee should exercise appropriate discretion when using social networks for personal and professional communications with friends, colleagues, parents, former students, etc. with the knowledge that adult behavior on social networks may be used as a model by our students. Be aware that what your write or post leaves a long-lasting, even permanent, record that potentially can be seen by students, their families, and other members of the St. Francis Xavier Catholic School System community. People can draw conclusions, however erroneous, based on online activities, which may affect their perceptions of that employee's professionalism. Photos and videos that are tagged by others may be available to anyone searching social networks. Nothing is truly private when posted online.

ST. FRANCIS XAVIER Catholic School System

101 E Northland Avenue
Appleton, WI 54911
MAIN 920.735.9380
FAX 920.735.1787

9. An employee should accept social network friend-requests from alumni only if they are over the age of 18. Discretion and good judgment is strong advised when communicating with alumni who may still have siblings in school and may be connected with current students. It is advised that you do not initiate friend contacts with alumni. Understand that the uneven power dynamics of the school, in which adults have authority over former students, continues to shape those relationships.
10. Employees should remind all other members of their network of their position as an educator or employee of the St. Francis Xavier Catholic School system, whose profile may be accessed by current or former students, so that these other members will monitor their posts to the network accordingly.
11. Employees should associate with social networking groups consistent with healthy, appropriate activities and the mission and reputation of the school.
12. Employees should exercise care with privacy settings and profile content. Content should be placed thoughtfully and periodically reviewed to maintain this standard.
13. Faculty who use social networks should do so using their own name, not a pseudonym or nickname. Conduct yourself online according to the same standards of honesty, respect, and morality that you would at school.
14. If an employee makes reference to the system or school by name or other means, they must include a disclaimer within their personal and professional blogs and other media that the views are their own and do not reflect on the St. Francis Xavier Catholic School system. For example, *"The postings on this site are my own and don't necessarily represent the positions or opinions of the St. Francis Xavier Catholic School System."* In spite of this, your views and opinions still reflect on this institution. Public statements should be in accord with our philosophy and beliefs.
15. Employees are to consult the "no photographs" list before posting images of students.
16. Using, transmitting or posting images of administrators, colleagues, parents or any other person without specific permission is prohibited.
17. Users should not use school technologies for illegal activities or to pursue information on such activities. It is forbidden to store or access illegal, inappropriate, or obscene material on school owned electronic equipment.
18. Users are not to use school technology for political lobbying for personal issues although communication may be made with politicians if it is curriculum-related.

GENERAL GUIDELINES FOR STUDENTS

1. Social media reaches audiences far beyond the school community. Students must use social sites responsibly and be accountable for their actions.
2. Students must follow the school code of conduct themselves online as they are expected to in school.
3. Social media venues are public and information can be shared beyond your control. Be conscious of what you post online as you will leave a long-lasting impression on many difference audiences.
4. Do not post or link anything (photos, videos, web pages, audio files, forums, groups, etc.) to your social networking sites that you wouldn't want friends, peers, parents, teachers, college admissions officers, or future employers to access. What you present on social networking forums represents you forever.
5. Only accept social network invitations form people you know. Utilize privacy settings to control access to your network, web pages, profiles, posts, blogs, wikis, podcasts, digital media, forums, groups, etc.
6. Do not misrepresent yourself by using someone else's identity.
7. Users should not use school technologies for illegal activities or to pursue information on such activities. It is forbidden to store or access illegal, inappropriate, or obscene material on school owned electronic equipment.
8. Students are only allowed to use cell phones or other personal digital devices according to the rules of his/her campus.
9. Students should never trespass into others user's folder or files.
10. Students are not to use school technology to access games, Facebook, or other social media sites without the approval of a teacher or administrator. Using unapproved sites during class time without permission is even a more serious offense.
11. Users are not to use the school technology for political lobbying or personal issues although communication may be made with politicians if it is curriculum-related.
12. Using, transmitting or posting images of administrators, teachers, staff, parents, other students, or any other person without specific permission is prohibited.
13. Students should never use electronic communication to gossip or spread false information (i.e. defame, libel) about administrators, teachers, staff, parents, other students, or any other person.

ST. FRANCIS XAVIER Catholic School System

101 E Northland Avenue
Appleton, WI 54911
MAIN 920.735.9380
FAX 920.735.1787

14. Photos or videos that are tagged by others may be available to anyone searching social networks. Nothing is truly private when posted online.

NETIQUETTE

1. Always abide by the generally accepted rules of network etiquette (netiquette).
2. Be polite in your messages. Use appropriate language and remember that you are a representative of our school and system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language.
3. Use and share computer resources courteously and efficiently.
4. If responding to someone with whom you disagree, remember to be respectful. Make sure that criticism is constructive and not hurtful. Do not use profane, obscene, or threatening language.

PRIVACY

1. There is not absolute right to privacy when using the school's technology resources. School personnel may review files and communications to maintain system integrity and ensure that users are using the system responsibly and appropriately. Authorized personnel will have the right to review any and all material saved, transmitted, accessed, or momentarily in use by the user. Users should not expect that files will be private.
2. All activity over the school network or using system technologies may be monitored and retained.
3. Any information contained or placed on the school's computer hard drive or the school's computer disks are the property of the school.

COPYRIGHT & PLAGIARISM

1. Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the internet should be appropriately cited, giving credit to the original author.
2. Users are to respect the right of intellectual property of other people and to respect all copyright laws. If a user is unsure whether copyright laws are being respected, they need to raise the question with the staff member with this expertise.

CYBERBULLYING

1. Cyberbullying is considered an act of harassment and will not be tolerated. Harassing, dissing, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send e-mails or post comments with the intent of scaring, hurting, or intimidating someone else.
2. Users should never post false information or engage in personal, prejudicial, or discriminatory attacks.
3. Engaging in cyberbullying behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime in which case, police will be involved. Remember that your activities may be monitored and retained.

SAFETY

1. Online stalkers and identify thieves are a real threat. Never share personal information, including, but not limited to, social security numbers, phone numbers, addresses, exact birthdates, financial information, and pictures with people you don't know or on unsecure sites.
2. Users should never agree to meet someone they meet online in real life without parent permission.
3. Users should recognize that among the valuable content that is available on line there is also unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the internet and report inappropriate content to an adult.
4. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety or if you feel violated, harassed, uncomfortable or accosted through the school's technology resources, bring it to the attention of an adult (teacher or staff if you're at school; parent if you using the device at home) immediately.

SECURITY

1. Users should keep their passwords secure and never share passwords with others. If someone tampers with your accounts without you knowing about it, you could be held accountable.
2. Users of the district network or other technologies are expected to alert technology staff immediately of any concerns for safety or security or any problem with its operation.
3. Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or program and not opening files or programs of unknown or untrusted origin.
4. If you believe a computer or mobile device you are using might be infected with a virus, you need to alert the technology staff immediately. Do not attempt to remove the virus yourself or download any programs to help remove the virus.
5. Users are not to try to find ways to circumvent the school's safety measures and filtering tools.

ST. FRANCIS XAVIER Catholic School System

101 E Northland Avenue
Appleton, WI 54911
MAIN 920.735.9380
FAX 920.735.1787

6. Users are not to attempt to hack or access sites, servers, or content that isn't intended for their use.

DAMAGE AND VANDALISM

1. Students should never tamper with or vandalize the property of the school or other users including equipment; cabling and other infrastructure; any security system that protects the school's computer resources; and data. Users are not to tamper with, remove components from, or otherwise deliberately interfere with the operation of computers, networks, printers, or other associated peripherals.
2. Vandalism is further defined, but not limited to, deleting, examining, copying, or modifying files, data, e-mail or voice mail belonging to other users, and/or attempts of same; attempts to breach security codes and/or passwords; and/or destruction, abuse or modification of computer hardware and/or software including changes to preferences, and/or attempts of same.
3. The St. Francis Xavier Catholic School System will not be held liable for any damage, loss, or theft of any personal property brought to school, including technology devices.

CONSEQUENCES

Users need to recognize that the use of school technology is a privilege and not a right and should treat is such. Students are expected to follow the same rules for good behavior and respectful conduct online as offline. Misuse of school resources can result in disciplinary action.

1. The system maintains the right to confiscate and search any cell phone or other personal electronic device found on school premises or used at school.
2. The system reserves the right to discipline student for conduct, whether inside or outside school, that is detrimental to the reputation of the school or system.
3. Violations of this policy may have disciplinary repercussions for students, including suspension of network, technology, or computer privileges; payment for any damages caused; detention, suspension or expulsion from school and school-related activities; and legal action and/or prosecution.
   Violations of this policy may have disciplinary repercussions for employees and adult volunteers, including payment for any damages caused; suspension or termination of job; and legal action and/or prosecution.

Information from the following schools was used as source for this policy:

The Castilleja School	http://www.castilleja.org/
The Urban School	http://www.urbanschool.org/
Jackson-Madison County School System	http://www.jmcss.org/
Greenburg Central Catholic High School	http://www.gcchs.org/
Catholic Schools of the Archdiocese of Philadelphia	http://archpila.org/
Rosendale-Brandon School System	http://www.rbsd.k12.wi.us/
Judge Memorial Catholic High School	http://www.judgememorial.com/
Salpointe Catholic High School	http://www.salpointe.org/

Article "Technology Related Communication between Adults and Students: by Robert Hugh Farley.

ST. FRANCIS XAVIER
Catholic School System

101 E Northland Avenue
Appleton, WI 54911
MAIN 920.735.9380
FAX 920.735.1787

ST. FRANCIS XAVIER ACCEPTABLE USE POLICY (AUP)

Students and Parents

I have read, understand, and agree to abide by this Acceptable Use Policy of the St. Francis Xavier Catholic School System.

Note: Parents should be aware that technology devices that tap into the wireless network of a Xavier campus will receive a filtered internet. Students using a device that receives internet through a 3G or 4G network will not be filtered by the school. Contact your internet provider to learn how to provide a filtered internet for your student.

Complete the following for student(s) attending this campus. Please return this form to your campus principal.

Student Name _____

Student Signature _____ Date _____

Student Name _____

Student Signature _____ Date _____

Student Name _____

Student Signature _____ Date _____

Student Name _____

Student Signature _____ Date _____

Student Name _____

Student Signature _____ Date _____

Student Name _____

Student Signature _____ Date _____

Parent Name(s) _____

Parent Signature _____ Date _____

****

Employee Name _____ **Campus** _____

Employee Signature _____ Date _____