

Guidelines for School Policies and Procedures

Acceptable Use Policies, Internet Safety curriculum, Social Media

Background and Introduction:

Electronic devices and technology are important educational tools that allow teachers to access information, differentiate instruction, integrate content and communicate directly with both students and parents. These tools are used by various segments of the school community including: teachers, students, administrators and parents. While digital tools share a common origin, they allow varied methods of communication including: e-mail, texting, messaging, social media, blogs, wikis, and others. As this type of communication continues to evolve and grow, and as it is used both for professional learning, instructional and personal purposes, and as such technology is procured, owned and operated both by schools and individual students for separate though often intersecting purposes, it is necessary to have clear guidelines and policies governing the appropriate use of and interaction with such technology both for school staff and students.

Toward this end a group of committed Catholic educators assembled in May 2015 to discuss the varied uses of technology and recommend guidelines after which Catholic schools in the Diocese of Madison might pattern their own acceptable use policies. The following guidelines are a result of this work. While there will never be a perfect, all encompassing, Acceptable Use Policy (AUP), as technology will continue to change and expand, these guidelines represent current best practice and are meant to serve as a template and resource to schools in developing their own AUPs and technology policies.

The Office of Catholic Schools wishes to express its gratitude to the members of the committee who gave freely of their time and expertise to create these guidelines. Those persons are:

Elizabeth First -	Blessed Sacrament Catholic School, Madison
Nikki Nemitz –	St. Clement Catholic School, Lancaster
Carla Pool -	St. Dennis Catholic School, Madison
Kara Roisum -	St. Ann Catholic School, Stoughton
Mary Jo Vitale -	Our Lady Queen of Peace Catholic School, Madison

Philosophy of Acceptable Use for Students and Staff:

Use of technology by persons in Catholic Schools throughout the Diocese of Madison should support and facilitate excellence in all facets of Catholic education, thoughtfully embrace new avenues of learning and school operation, and advocate for media literacy and digital citizenship.

Policy Contents:

All Catholic schools in the Diocese of Madison must maintain an Acceptable Use Policy for both staff and students.

1. Such policies should address, but not be limited to the following:
 - User agreements for school-provided Internet and wi-fi access.
 - Restrictions of use of such Internet and wi-fi network.
 - User agreements for the use and maintenance of school-provided technology such as desktop computers, laptop computers, tablets (iPads, Chromebooks, Surface etc.) and any other personal, electronic devices (cell phones, iPods, Nooks, Kindles, Apple watches and other student owned devices that might be brought to school).
 - Clear consequences for violating said policy and/or regulations.
2. Due to the rapid pace of technological development in both the educational and public realm, these policies should be reviewed no less than once every two years. Such review should be conducted by the school principal and the parish Education Commission, or in the case of non-parish schools, a governing body similar to the Education Commission, school board, board of directors or sub-committee thereof.

While the Office of Catholic Schools (OCS) recognizes that situations in various schools and school communities differ widely, and whereas the OCS supports and promotes the principle of subsidiarity, or addressing issues at the most local level of those directly affected, schools retain and hold the autonomy to craft their own policies. However, as there are “best practices” that have been culled from extensive research and consultation with several other dioceses, technology staff and legal staff, the OCS offers the following recommendations and guidelines. These are illustrated in the sample policies and guidelines attached to this document. Schools should strive to follow this guidance as closely as possible, adjusting for the particular circumstances of their local situation. While reviews and revisions of school policies should be conducted at the local level, the Office of Catholic Schools remains available to offer advice and consultation in the review and revision process.

Schools are encouraged to vet their initial, proposed policy, as well as any future revisions, with local legal counsel. Diocesan attorneys are available to assist with this through the Office of Catholic Schools, however individual schools are expected to bear the cost of this service.

NOTE: Schools offering a 1:1 program will need to have a specific policy governing the use of the school-issued tablets or laptops. Edgewood High School of the Sacred Heart provides an extensive and detailed example of such a policy for Chromebooks, while Our Lady Queen of Peace provides an example for iPads. These may be viewed at the following links:

[2015-16 Edgewood Student Chrome Handbook](#)

[Queen of Peace 1:1 and Technology Acceptable Use Handbook 2015-16](#)

In addition to the sample policies and guidelines, resources and references are provided below.

RESOURCES:

- **National Center for Missing and Exploited Children**
 - <http://www.netismartz.org>
 - Provides excellent resources for students, parents, and teachers about staying safe when you're online. Emphasis is placed on safe behavior, guarding personal information and proper interactions with others online. Training materials are available for schools.

- **Federal Communications Commission (FCC) – Children's Internet Protection Act (CIPA)**
 - <https://transition.fcc.gov/cgb/consumerfacts/cipa.pdf>
 - Explains the rationale and highlights of CIPA and what schools receiving federal funds under E-Rate must do to comply with the law.

- **Net Cetera: Chatting with Kids About Being Online**
 - <http://www.onguardonline.gov/articles/pdf-0001-netcetera.pdf>
 - Guideline for parents and teachers regarding teaching children to be safe online. It outlines what should be taught in school about acceptable use and online behavior. It is an excellent guide to share with parents so that safe and acceptable online practices are reinforced at home.

- **Onguard Online.gov**
 - <http://www.onguardonline.gov/>
 - An excellent resource that has special sections for teachers and parents. The teacher section has resources specifically target to students at various grade levels, classroom teachers and IT professionals in schools. It offers free classroom resources.
 - This resource is updated frequently and even contains information on the latest mobile apps and children's apps as well as tips on preventing cyberbullying.

- **Common Sense Education on E-Rate and CIPA: A Teacher's Guide**
 - <https://www.common sense media.org/educators/erate-teachers>
 - DPI recommended - contains free lesson plans for appropriate use and online safety as well as digital citizenship. (Be sure to scroll down the page to find these.)

- **CIPA, COPPA, Data Privacy and Digital Citizenship**
 - <http://dpi.wi.gov/imt/digital-learning-planning/Internet-safety>
 - DPI page containing multiple resources for teachers and parents. (Scroll to the bottom.)

Sample Handbook Statements:

General Statement of Expectation

Every faculty/staff handbook should contain the following statement or one that is substantially similar in meaning and expectation.

STUDENT/PARENT/FAMILY HANDBOOK:

Technology Usage: Each student/parent is expected to sign the Acceptable Use Policy agreement at the end of this Handbook. Students and parents must agree to abide by this policy before the student is allowed to use the school network and e-mail or use any school-owned electronic devices, including computers, laptops and tablets. It is expected that students at _____ Catholic School will conduct themselves, both on and off campus, when school is in session and out of session, in a manner that brings respect to themselves and the school. Use of computers/laptops, iPads/tablets, the school network and the Internet, are provided for academic use only. **The use of the Internet to send jokes, forwarded e-mail messages, or other communication not related to academic purposes is prohibited.** Transmission of such material may result in loss of computer privileges or other disciplinary measures. This includes, but is not limited to defamatory statements made on a student's webpage, blog, or social media regarding the administration, employees, teachers, students, or the parish.

TEACHER/EMPLOYEE HANDBOOK:

Technology Usage: Each teacher/employee is expected to sign an Acceptable Use Policy agreement and enforce this policy with his/her students (see Agreement at the end of this Handbook). Use of computers/laptops, iPads/tablets, the school network and the Internet, are provided for **professional use only**. **The use of the Internet to send jokes, forwarded e-mail messages, or other communication not related to the professional duties to which you are assigned is strictly prohibited.** Transmission of such material may result in loss of computer privileges or termination of employment. This includes, but is not limited to defamatory statements made on a teacher's/employee's webpage, blog, or social media regarding the administration, other employees, teachers, students, or the parish. Teachers should not "friend" their students on social networking sites. This is a breach of professional boundaries.

VOLUNTEER HANDBOOK:

Technology Usage: Any photographs or statements made on a volunteer's Social Networking Site may be cause for dismissal of services and separation of the volunteer's family from the school. This includes defamatory comments made about the school administration, other teachers, students, or the parish. Volunteers should never take photographs of students during school-sponsored activities. This includes, but is not limited to, field trips and class parties. All volunteers who use technology as part of their volunteer duties are expected to sign and abide by the Acceptable Use Agreement at the end of this handbook.

SAMPLE STAFF/FACULTY/VOLUNTEER AGREEMENT FOR TECHNOLOGY USE:

The access to, and the use of, the Parish/Schools' Internet and related technologies is made available to adult personnel within the parish and school. It will be provided only to those individuals who sign this Agreement. The signing of this Agreement indicates the party who signed has read the terms and conditions, voluntarily agrees to be bound by them, and understands their significance.

All uses of the Internet and related technology shall be for educational purposes or communication of school business. Personal communications may be allowed per parish/school policy, however, all employees are hereby notified that any communications sent using hardware, software, internal networks, routers, servers or other technological infrastructure belonging to the parish/school, are not private and furthermore that the nature and contents of such communications may be read and reviewed by parish/school authorities. Such communications bear no right or expectation of privacy and are fully discoverable by law.

The failure of any user to follow the terms and conditions hereof may result in the loss of privileges and/or disciplinary action.

The term *network* as used herein shall refer to any computer that is connected to another to share information, a printer, or other input or output devices, intranet, Internet, the School/Parish web sites, and the use of e-mail.

TERMS AND CONDITIONS**1. Acceptable Use**

Access and use of the School/Parish network and technology resources must be only for the purpose of education, research or communication and then be consistent with the terms of this Agreement, as well as the educational and moral criteria and objectives of the School/Parish.

2. Privacy

The user does not have any right of privacy whatsoever in relation to his/her use of the network and/or email. Consequently, all electronic and telephone communication systems and all communication and information transmitted by, received from, or stored in any manner are the property of the School/Parish and are to be used for educational purposes only. To ensure that the use of the network is consistent with the educational objectives and philosophy of the School/Parish, authorized representatives may monitor the use of the network from time to time, which may include the printing and reading of all information stored and all e-mails entering, leaving or stored, and all files created and saved in the system. The system administrator may remove any material stored by the users which violates the terms of this agreement.

3. **Privilege/Relegation**

The use of the School/Parish network, and other related technology, is a privilege being offered for educational purposes, and any inappropriate use or any use inconsistent with this Agreement or inappropriate with the educational and moral objectives of the Diocese, Parish, and School, may result in cancellation of the privilege. The principal, pastor, superintendent (the “Administrator”) will make all decisions regarding whether or not the user has violated this Agreement and may deny, revoke, or suspend access at any time. The decision of the Administrator is final.

4. **Network Code of Conduct**

Users are expected to abide by the following rules:

Adult personnel act as representatives of the school reflecting the mission and philosophy of the School and Parish.

The network shall not be used in any way that would disrupt its functionality for others.

The personal address, phone number, or social security number of any student, staff person, faculty members, or colleagues should not be revealed when using the Internet or network.

The network may not be used for personal business, financial gain, or the purchase of merchandise or services without authorization.

Material downloaded from the Internet or email is to be scanned for viruses.

No employee or volunteer may install any software without the prior approval of the System’s Administrator or Principal.

No user may install any program files obtained from another computer without the prior approval of the System’s Administrator or Principal.

Data that is composed, transmitted, accessed or received via the network must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation or any other characteristic protected by law.

The unauthorized use, installation, reproduction or distribution of copyrighted, trademarked or patented material on the network is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it, nor has received or procured authorization for its use, that material may not be put on the

network. Employees are also responsible for ensuring that the person sending any material over the network has the appropriate distribution rights.

The following behaviors are examples of **previously stated** or additional actions and activities that are prohibited and may result in disciplinary action:

- Sending or posting discriminatory, harassing or threatening messages or images
- Stealing, using or disclosing someone else's code or password without authorization
- Copying, pirating or downloading software and electronic files without permission of the manufacturer or developer
- Violating copyright law
- Failing to observe licensing agreements
- Engaging in unauthorized transactions that may incur a cost to the school or initiating unwanted Internet services and transmissions.
- Sending or posting messages or material that could damage the School/Parish/Diocese's image or reputation or damage, defame or slander the reputation of an individual associated with the School/Parish.
- Participating in the viewing or exchange of pornography or obscene materials
- Using the network for unauthorized political causes or activities, religious activities or personally engaging in any sort of gambling
- Jeopardizing the security of the organization's electronic communications systems
- Engaging in any other illegal activities
- Using the network to engage in conduct which is contrary to the teaching and philosophy of the Roman Catholic Church. The Diocesan Ordinary will be the final interpreter of what conduct is contrary to the teaching and philosophy of the Roman Catholic Church.

5. Web Pages

It is the intent of _____ Catholic School to publish web pages as a method of providing information about the business of the School. This may include the posting of meetings, agendas, students' activities, projects and accomplishments, schedules and other information of interest to students, parents and the community. Classrooms may participate in the development of web pages as on-going educational projects.

Disclosure of student information on any web page will be limited to first name and last initial. Photographs or video of students may be posted on the School website: however, no photograph or video of any student will be captioned with the student's name, or identify the student by name in any other manner. No image of a student may be posted in such a way that the image of that student may be matched up with the student's name.

Disclosure of the personal address, phone number or social security number of any student, staff person, faculty member or colleague is prohibited. Only school contact information should be made available.

The principal or her/his designee shall monitor all materials published on the Internet. The posting of any material that may violate copyright law is expressly prohibited.

6. **Guidelines for Using Social Media and Educational Networking Sites**

Social networks are rapidly growing in popularity and use by all ages in society. As staff/volunteer, we have a professional image to uphold and how we conduct ourselves online impacts this image. Educators' online identities are very public and can cause serious repercussion if their behavior is careless.

When using social networking sites:

- NEVER accept students as "friends" on personal social networking sites. Decline any student-initiated friends' requests.
- Do not initiate a "friends" request with students.
- Remember that people classified as "friends" have the ability to download and share your information with others.
- Post only what you want the world to see. Imagine your students, their parents, your administrator, visiting your site. On a social networking site, basically once you post something it may be available, even after it is removed from the site. Once something is posted you have no right to privacy.
- Do not discuss students or coworkers or publicly criticize school, parish or diocesan policies or personnel.
- Visit your profile's security and privacy settings. At a minimum, educators should have all privacy settings set to "only friends."

When using educational networking sites:

- Inform your Principal, fellow teachers and parents about your educational network and all applicable rules for network participants.
- The code of conduct applies to all use of educational/professional networking sites.
- When available, use school-supported networking tools.

- Do not say or do anything that you would not say or do as a teacher in the classroom. (Remember that all online communications are stored and can be monitored.)
- Have a clear statement of purpose and outcomes for the use of the networking tool.
- Establish a code of conduct for all network participants.
- Do not post images that include students without parental release forms on file.
- Pay close attention to the site's security settings and allow only approved participants access to the site.

7. **Hand-held Devices**

The use of hand-held devices is for educational and business purposes only. All rules of conduct apply. The School accepts no responsibility for loss or damage to those hand held devices brought into the School.

8. **Vandalism**

Vandalism is defined as any attempt to harm or destroy or the actual harm or destruction of data of another user, or to damage hardware or software. This includes, but is not limited to, the uploading or creation of computer viruses, or worms or other files or programs that damage, delete or modify data or applications.

9. **Indemnification**

The user hereby agrees to indemnify the School/Parish for any losses, costs, or damages, including attorney's fees, incurred by the School, Parish, or Diocese relating to or arising out of the user's breach of, or the enforcement of this Agreement or the School/Parish's enforcement thereof.

10. **Financial Obligations**

The employee or volunteer agrees to be responsible for any financial obligation incurred through the use of the network that is contrary to the terms of this agreement.

11. **No Warranty**

The School/Parish makes no warranties of any kind, whether expressed or implied, for the network service it is providing, and will not be responsible for any damages users suffer. This includes the loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions. The School/Parish further does not warrant, and has no responsibility, for the accuracy or quality of information obtained through the use of the network.

SAMPLE STAFF/FACULTY/VOLUNTEER AGREEMENT FOR TECHNOLOGY USE

I, an, employee, volunteer at _____, have read and understand and agreed to abide by the terms of this Agreement. I further understand and agree that should I breach any of the terms of this Agreement, my access privileges may be revoked, disciplinary action taken, and appropriate legal action may be taken. I further agree to be responsible for any cost or damages associated with, or resulting from, any breach of this Agreement, including attorney’s fees.

I, further, hereby release the School/Parish and its board members, employees, and agents from any claims or damages arising from my use, or inability to use the network, systems, or equipment, and arising from my use of the network in violation of this Agreement.

Employee/Volunteer Name (Please Print)

Employee/Volunteer Signature

Date

SAMPLE ACCEPTABLE USE AGREEMENT: STUDENTS/PARENTS

Adapted from NCEA's From the Chalkboard to the Chatroom.

As a computer user, I agree to follow the rules and code of ethics in all of my work with computers while employed or volunteering at _____ School:

1. I recognize that all computer users have the same right to use the equipment; therefore, I will not use the computer resources for non-academic purposes. I will not waste or take supplies such as paper, printer cartridges, and discs that are provided by the school. When I am in the computer lab, I will talk softly and work in ways that will not disturb other users. I will keep my computer work area clean and will not eat or drink in the computer lab.
2. I recognize that software is protected by copyright laws; therefore, I will not make unauthorized copies of software and I will not give, lend, or sell copies of software to others. I understand that I will not be allowed to bring software applications, games, or CD-ROMs from home to be used on school equipment without proof of licensure and prior approval of appropriate school personnel.
3. I recognize that the work of all users is valuable; therefore, I will protect the privacy of others by not trying to learn their password; I will not copy, change, read, or use files from another user without prior permission from that user; I will not attempt to gain unauthorized access to system programs for computer equipment; I will not use computer systems to disturb or harass other computer users or use inappropriate language in my communications.

I will honor my school's procedures for the storage of information. I realize that after prior notice has been given to me, files may be deleted from the system to protect the integrity of the network or because of space limitations on the computer's hard drive.

4. Each student who received Internet access will be instructed in the proper use of the network. The use of the Internet must be in support of education and research consistent with the educational objectives of the school. Students using network or computing resources must comply with the appropriate rules for that network or resource.

As a user of a network, I will not use bulletin boards or chat rooms. In addition, I will not reveal my personal information, home address, or personal phone number or those of students, teachers, or other staff members. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. The use of school computers and networking resources for commercial activities is not permitted. Their use for product advertisement or political lobbying is also prohibited.

5. Parents must realize that although the school utilizes filters to minimize the possibility of student exposure to inappropriate material, no filtering system is foolproof, and students may encounter material on a network/bulletin board that is not considered appropriate (vulgar jokes, statements of belief that some might consider immoral, etc.) The student is responsible for not pursuing material that could be considered offensive. Pursuit of such material will result in loss of technology privileges and/or other disciplinary measures.

6. The use of the computer is a privilege, not a right, and inappropriate use will result in the cancellation of these privileges. Vandalism or intentional modification of system settings will result in cancellation of privileges and/or school disciplinary action. The school reserves the right to seek financial restitution for any damage caused by a student or other user. The system administrators will deem what is inappropriate use, and their decision is final. The administration, faculty, and staff of the school may request that the system administrator deny, revoke, or suspend specific user privileges. Violations of the rules and code of ethics described above will be dealt with seriously.

Technology Concerns

Blogs: Engagement in online blogs such as, but not limited to Facebook®, etc. may result in disciplinary actions (including expulsion) if the content of the student’s or parent’s blog includes defamatory comments regarding the school, the faculty, other students or the parish.

Cell Phones: If a student needs a cell phone after school due to walking home from school, entering a house where no one is home, or attending sport practices or games, he/she should bring the cell phone to the office upon arrival in the morning to park the cell phone in the off position for the day. The cell phone may be picked up by the student at dismissal. At no time during the day should a cell phone be in a student’s locker or in his/her possession. **Items taken away from students will be returned to the parent(s)/guardian(s) on the last day of the school year.**

Children’s Internet Protection Act (CIPA):

It is the policy of _____ School to make a good faith effort to:

(a) prevent user (student, staff, minor, adult) access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications.

(b) prevent unauthorized access and other unlawful online activity.

(c) prevent unauthorized online disclosure, use, or dissemination of personal identification of minors.

(d) comply with the Children’s Internet Protection Act [Public Law No. 106-554 and 47 USC 254(h)].

(e) educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying

awareness and response. (Public Law No: 110-385 Protecting Children in the 21st Century Act)

To the extent that it is practical, technology protection measures (or “Internet filters”) shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Realizing that no Internet filter device is 100% effective, _____ School shall make every effort to maintain effective filtering continuously. The School acknowledges that the potential exposure to inappropriate information is not and cannot be entirely avoided.

Personal Digital Devices and Electronic Readers (E-readers): Electronic readers, simply called “e-Readers”, are digital devices that can store books, periodicals, magazines, and other electronic media. e-Readers like Amazon’s Kindle®, Barnes & Noble’s Nook®, Apple’s iTouch® or iPod®, as well as tablets such as Surface®, iPad® and Apple Watch® are quickly becoming ubiquitous in our digital culture and they simply cannot be ignored. _____ Catholic School, in striving to maintain technological relevance in education, is providing the opportunity for students to use these devices in accordance with our Device Acceptable Use Policy. This opportunity is a privilege that requires extra caution and responsibility both on the part of the students and their parents.

NOTE: Schools may opt to prohibit students from bringing their own personal digital devices and restrict them to use only school-issued devices (Chrome Books®, iPads® etc.) at their discretion. The following guidelines are provided for schools opting to allow these devices.

Device Acceptable Use Policy:

The wide variety of hardware and software capabilities of available e-Readers/tablets makes them challenging to monitor and control in a school environment in contrast with school-owned technology assets like computers, etc. Therefore, our e-Reader Acceptable Use Policy needs to be specific and clear. A student who violates any portion of the Device Acceptable Use Policy may immediately lose the privilege to use their device at school for a length of time commensurate with the nature of the violation.

1. All personal digital devices must be registered with _____ Catholic School’s IT Specialist/Principal and accompanied by the Acceptable Use Agreement Form signed both by the parents and the student.
2. Personal digital devices are to be used **only** for the reading of school approved material (books, etc.) and not for other purposes such as communication, entertainment, music, gaming, etc.
3. All material on the personal digital device must comply with the spirit and policies of _____ Catholic School. Please refer to the Parent-Student Handbook for more details.

4. All personal digital devices must have cellular and network capabilities disabled (turned off) while the device is at school.
5. Personal digital devices may be used only at appropriate times in accordance with teacher instructions. The device must not be a distraction for the student or those around him/her nor be a source of any classroom disruption.
6. Personal digital devices are not to be used during lunch, middle-school breaks, or during playground/recess time.
7. The student is responsible for knowing how to properly and effectively use their personal digital device. The school will not and is under no obligation to provide support for personal digital devices.

Instagram®: Photos and captions on a student or parent’s Instagram® account that depict the school, the faculty, other students, or the parish in a defamatory way or that depict bare parts of the body that would normally be clothed, or depict pornographic images, will result in disciplinary action.

Sexting: Students involved in possession or transmission of inappropriate photos of others or themselves on their cell phones or other electronic devices face suspension and/or expulsion.

Texting: Students should at no time be involved in texting during the course of the school day. Students involved in texting at school face detention, suspension and/or expulsion.

Virtual Reality Sites: Virtual Reality Sites such as, but not limited to, www.there.com® and www.secondlife.com®, etc. pose a developmental and moral risk to the life of a student. Parents are cautioned to be aware of the online sites visited by their children, knowing that often predators are not living in a neighborhood, but within the home via a computer. Students or parents whose avatars depict other students, teachers, or parish staff in a defamatory light face detention, suspension, or expulsion.